

Základní škola, Praha 8, Žernosecká 3

SMĚRNICE PRO POUŽÍVÁNÍ SYSTÉMŮ UMĚLÉ INTELIGENCE (AI) VE ŠKOLSTVÍ

Pořadové číslo – číslo jednací:

122 – POR/03/2026

Pedagogická rada projednala dne:

31. 8. 2026

Zpracoval:

JUDr. Eva Janečková

Schválil:

RNDr. Božena Čerňanská, Ph.D.

Směrnice nabývá platnosti ode dne:

2. srpna 2026

Změny v organizačním řádu jsou prováděny formou číslovaných písemných dodatků, které tvoří součást tohoto předpisu.

Obsah

1. Účel, právní rámec a školský kontext směrnice.....	5
1.1 Právní rámec	5
1.2 Zvláštní citlivost školského prostředí	5
2. Právní následky porušení směrnice.....	6
3. Definice pojmů a role školy podle AI Act.....	6
3.1 Role školy: implementátor, poskytovatel, správce a zpracovatel	6
4. Riziková kategorizace AI ve škole podle AI Act.....	7
4.1 Vysoce rizikové systémy ve vzdělávání	7
4.2 Zakázané praktiky zvlášť významné pro školu.....	7
5. Zásady odpovědného používání AI ve škole	8
5.1 Pravidlo „žádné osobní údaje do veřejné AI“	8
5.2 Pravidlo „AI nikdy sama nerozhoduje o žákovi“	8
6. Používání AI nástrojů učiteli, zaměstnanci a žáky	8
6.1 Používání nástrojů typu ChatGPT, Copilot a obdobných asistentů zaměstnanci	8
6.2 Překladače a jazykové nástroje	9
6.3 Používání AI žáky.....	9
6.4 Zakázané jednání žáků.....	9
7. AI ve výuce, domácí přípravě, písemných pracích a hodnocení.....	9
7.1 Pedagogické použití AI.....	9
7.2 AI v hodnocení.....	10
7.3 AI detektory a akademická integrita	10
8. Automatizované systémy, studijní systémy, hodnocení a analýzy dat	10
8.1 Příklady automatizace a požadovaný režim.....	10
8.2 Zásady pro analýzu studijních dat.....	10
8.3 Minimální dokumentace automatizovaného systému	11
9. Chatbot na webu školy a AI v komunikaci se žáky a rodiči	11
9.1 Povolené a zakázané použití chatbotu	11
9.2 Transparentnost chatbotu	11
9.3 Provozní a bezpečnostní požadavky	11
10. Kamerové, přístupové, dohledové a biometrické systémy	12
10.1 Zákaz detekce emocí a citlivé biometrické kategorizace	12
10.2 Rozpoznávání obličejů a biometrická docházka	12
10.3 AI proctoring a dohled při zkouškách.....	12
10.4 Kamerová analytika v prostorách školy.....	12
11. Práce s osobními údaji žáků, uchazečů, rodičů a zaměstnanců	12
11.1 Kategorie údajů se zvýšenou ochranou.....	12
11.2 Právní základy a souhlas.....	13
11.3 DPIA, FRIA a posouzení dopadů	13

11.4 Zákaz používání vstupů pro trénink mimo kontrolu školy	13
12. Interní správa AI, schvalování, evidence a odpovědnosti.....	13
12.1 Schvalovací proces	13
12.2 Evidence AI systému	13
12.3 Vymezení odpovědnosti.....	14
12.4 Nákup a smluvní požadavky	14
13. Transparentnost vůči žákům, rodičům a ochrana práv žáků	14
13.1 Minimální obsah informační povinnosti	14
13.2 Práva žáků.....	15
13.3 Ochrana zranitelných skupin a přístupnost	15
14. Zakázané způsoby použití AI a zvláštní omezení ve školství.....	15
15. Pravidla kontroly používání AI a akademické integrity	15
15.1 Kontrola zaměstnanců.....	15
15.2 Kontrola žáků a podezření na nepovolené použití AI.....	16
15.3 Dokumentace kontroly	16
16. Požadavky na ochranu osobních údajů a informační bezpečnost u AI systémů	16
16.1 Minimální schvalovací kritéria	16
16.2 Provozní povinnosti	16
16.3 Bezpečnostní minimum pro AI nástroje	16
17. Vlastnictví obsahu, autorská práva, citace a označování AI výstupů	17
17.1 Výukové materiály.....	17
17.2 Žákovské práce a přiznání použití AI	17
17.3 Označování syntetického obsahu	17
18. AI gramotnost, školení a metodická podpora	17
18.1 Povinné okruhy školení zaměstnanců.....	17
18.2 Role-based školení.....	18
18.3 Evidence školení	18
19. Incidenty, stížnosti, nápravná opatření a revize směrnice.....	18
19.1 Incidenty	18
19.2 Stížnosti a námitky.....	18
19.3 Revize směrnice.....	18
Příloha č. 1: OnePager – 12 pravidel bezpečného a odpovědného používání AI ve škole	19
Příloha č. 2: Quick Guide pro každodenní rozhodování	20
Kontrolní otázky před použitím AI.....	20
Příloha č. 3: Karta AI systému / schvalovací formulář	21
Příloha č. 4: Checklist DPIA/FRIA pro AI ve školství.....	22
Příloha č. 5: Vzor informačního oznámení pro žáky a zákonné zástupce	23
Doporučený krátký text pro web nebo LMS.....	23
Příloha č. 6: Vzor záznamu o kontrole používání AI.....	24

Příloha č. 7: Potvrzení zaměstnance o seznámení se směrnicí.....	25
Doporučení k evidenci	25

1. Účel, právní rámec a školský kontext směrnice

Tato směrnice upravuje pravidla pro pořizování, vývoj, zavádění, testování, provoz a každodenní používání systémů umělé inteligence (AI) v prostředí **Základní škola, Praha 8, Žernosecká 3** (dále jen „škola“). Navazuje na obecnou interní směrnici pro používání AI, ale rozšiřuje ji o zvláštní rizika školství, zejména dopady AI na právo na vzdělání, rovné zacházení, hodnocení žáků, ochranu dětí a mladistvých, soukromí, akademickou integritu a důvěru v rozhodování školy.

Směrnice má umožnit bezpečné, přiměřené a pedagogicky účelné využívání AI nástrojů, například při přípravě výuky, dostupnosti studijních materiálů, jazykové podpoře, individualizované zpětné vazbě, administrativní podpoře a komunikaci se žáky a zákonnými zástupci. Současně stanoví hranice pro použití AI tam, kde by mohlo dojít k nepřiměřenému zásahu do práv žáků, k diskriminaci, netransparentnímu hodnocení nebo neodůvodněnému sledování.

Směrnice se vztahuje na pedagogické i nepedagogické zaměstnance, vedení školy, externí vyučující, členy komisí, administrativní pracovníky, ICT správce, dodavatele jednající jménem školy a v přiměřeném rozsahu také na žáky, zákonné zástupce a další osoby, které používají AI v souvislosti s činností školy, školním účtem, školním informačním systémem, školní sítí nebo školou zadaným úkolem.

Pro žáky se tato směrnice použije zejména jako pravidlo akademické integrity, pravidlo používání školních ICT prostředků a pravidlo plnění výukových povinností. Má-li být pravidlo vůči žákům vynucováno disciplinárně nebo v rámci hodnocení, musí být odpovídajícím způsobem promítnuto do školního řádu.

1.1 Právní rámec

Směrnice je vykládána a aplikována zejména v souladu s nařízením (EU) 2024/1689 o umělé inteligenci (AI Act), nařízením (EU) 2016/679 (GDPR), zákonem č. 110/2019 Sb., zákonem č. 561/2004 Sb. nebo příslušnými vysokoškolskými a sektorovými předpisy, právními předpisy v oblasti pracovního práva, autorského práva, kybernetické bezpečnosti a vnitřními předpisy školy.

AI Act se na školu typicky vztahuje v roli „nasazovatele“ (deployer), pokud škola používá AI systém pod svou autoritou v rámci profesní nebo veřejné činnosti. Pokud škola AI systém sama vyvíjí, podstatně upravuje, uvádí pod svým názvem nebo mění jeho určený účel, může se v konkrétním případě dostat také do role poskytovatele nebo jiné osoby v hodnotovém řetězci AI.

Právní stav a časová účinnost povinností podle AI Act je nutné průběžně ověřovat. Tato směrnice je nastavena konzervativně: i tam, kde jsou některé povinnosti AI Act účinné později nebo se jejich výklad vyvíjí, škola postupuje tak, aby měla předem připravenou evidenci AI, transparentní pravidla, lidský dohled a posouzení dopadů na práva žáků.

1.2 Zvláštní citlivost školského prostředí

Školské prostředí je z hlediska AI zvláště citlivé, protože rozhodnutí a doporučení školy mohou ovlivnit přístup ke vzdělání, průběh studia, známky, kázeňská opatření, doporučení podpůrných opatření. Řada dotčených osob je nezletilá nebo se nachází ve vztahu závislosti na škole. Škola proto nesmí používat AI jen proto, že je technicky dostupná; každé použití musí být účelné, přiměřené, kontrolovatelné a vysvětlitelné.

Oblast	Typické riziko ve škole	Minimální požadavek směrnice
Výuka a příprava materiálů	Nepřesný nebo zaujatý výklad, chybný zdroj, skrytý vliv na obsah výuky.	Učitel provede odborný přezkum, označí významné AI použití a neuvede AI výstup jako ověřený fakt bez kontroly.
Hodnocení a přijímání	Zásah do práva na vzdělání, diskriminace, netransparentní rozhodnutí.	AI nesmí sama definitivně rozhodovat; nutný lidský přezkum, dokumentace a možnost obrany.
Analýza dat a predikce	Profilování žáků, stigmatizace, chybné predikce rizika neúspěchu.	DPIA/FRIA podle rizika, minimalizace dat, role-based přístup a zákaz nepřiměřeného profilování.
Kamery a přístupové systémy	Skryté sledování, biometrie, detekce emocí nebo chování.	Oddělit běžné bezpečnostní systémy od AI analytiky; AI funkce použít jen po zvláštním posouzení.
Chatbot a komunikace	Halucinace, poskytnutí nesprávné rady, sběr osobních údajů.	Jasně označení AI, omezení na obecné informace, eskalace na člověka a kontrola znalostní báze.

2. Právní následky porušení směrnice

Porušení této směrnice se považuje za porušení pracovních, smluvních, studijních nebo interních povinností podle postavení dotčené osoby. Škola vyhodnocuje závažnost porušení individuálně s přihlédnutím k rozsahu a citlivosti dotčených dat, věku a postavení dotčených osob, míře zavinění, opakování jednání, vzniklé nebo hrozící újmě, dopadu na práva žáků a povaze použitého AI systému.

U zaměstnanců může porušení vést zejména k nápravným opatřením, omezení nebo odebrání přístupu k AI systémům, povinnému proškolení, zápisu do incidentního řízení, pracovněprávním opatřením, náhradě škody nebo k oznámení bezpečnostního či právního incidentu příslušným orgánům. U dodavatelů může být porušení řešeno smluvními sankcemi, pozastavením služby, požadavkem na audit, ukončením smlouvy nebo náhradou škody.

U žáků se postupuje přiměřeně podle školního řádu. Žák nesmí být sankcionován pouze na základě automatického výstupu AI detektoru nebo jiného automatizovaného indikátoru bez lidského přezkumu, možnosti vyjádření a přiměřeného ověření skutkového stavu.

Porušení spočívající v neoprávněném vložení osobních údajů žáků do veřejného AI systému, použití AI pro skryté sledování, manipulaci s důkazy, neoprávněné biometrické zpracování nebo automatizované rozhodování o žákovi bez lidského přezkumu se považuje za závažné porušení a musí být posouzeno také jako možný bezpečnostní incident, incident ochrany osobních údajů nebo porušení práv žáků.

3. Definice pojmů a role školy podle AI Act

Pojmy použité v této směrnici se vykládají v souladu s AI Act, GDPR, právními předpisy ve školství a účelem této směrnice. Pokud je výklad sporný, použije se přísnější režim ochrany práv žáků, ochrany osobních údajů, důvěrnosti a bezpečnosti.

Pojem	Výklad pro účely této směrnice
AI systém	Systém založený na strojovém učení, pravidlových, statistických, generativních nebo jiných algoritmičeských technikách, který s určitou mírou autonomie vytváří výstupy, jako jsou texty, překlady, doporučení, predikce, hodnocení, klasifikace, upozornění, rozhodnutí nebo analýzy ovlivňující výuku, administrativu, fyzické nebo virtuální prostředí školy.
Generativní AI	AI systém vytvářející nový text, obraz, zvuk, video, kód, prezentaci, test, řešení úlohy, překlad, shrnutí nebo jiný obsah na základě zadání uživatele nebo jiných vstupních dat.
Schválený AI systém	AI systém posouzený a písemně povolený školou pro konkrétní účel, kategorii dat, skupinu uživatelů, bezpečnostní režim a dobu použití. Schválení nástroje pro jeden účel neznamená schválení pro jiný účel, například pro hodnocení žáků.
Veřejný AI systém	AI služba dostupná veřejně nebo přes osobní účet, u níž škola nemá smluvně zajištěny požadavky na ochranu osobních údajů, zákaz použití vstupů pro trénink, auditovatelnost, správu účtů, mazání dat a odpovědnost dodavatele.
Žák	Pro účely směrnice žák a v přiměřeném rozsahu také zákonný zástupce nebo osoba, jejíž údaje jsou ve školním procesu zpracovávány.
Lidský dohled	Reálný, kvalifikovaný a dokumentovatelný dohled člověka nad použitím AI, včetně schopnosti porozumět účelu systému, zpochybnit výstup, zastavit použití, opravit chybu, převzít odpovědnost a umožnit dotčené osobě obranu.
Hodnocení žáků	Známkování, bodování, slovní hodnocení, posouzení splnění výstupů učení, přijímací řízení, doporučení studijní cesty, kázeňské posouzení, detekce podvodu, proctoring a jiné posouzení ovlivňující práva nebo oprávněné zájmy žáka.
Vysoce rizikové použití ve školství	Použití AI spadající pod Annex III AI Act nebo použití s obdobným dopadem na práva žáků, zejména přístup ke vzdělání, hodnocení výsledků učení, určení úrovně vzdělávání, monitoring zakázaného chování při testech, biometrické a dohledové systémy.
AI detektor	Nástroj, který odhaduje, zda text, obraz, kód nebo jiný výstup vytvořil člověk nebo AI. Je pouze podpůrným indikátorem, nikoli důkazem sám o sobě.

3.1 Role školy: implementátor, poskytovatel, správce a zpracovatel

Škola je při běžném používání nástrojů typu ChatGPT, Microsoft Copilot, překladačů, LMS funkcí, studijních analytik nebo chatbotu zpravidla implementátor AI systému. V této roli musí používat systém v souladu s jeho určeným účelem, pokyny dodavatele, interním schválením, právním rámcem a zásadami ochrany žáků.

Škola se může stát poskytovatelem AI systému, pokud systém sama vyvíjí, trénuje, uvádí pod vlastním názvem, integruje do své služby nebo podstatně mění jeho určený účel. Příkladem je vlastní algoritmus

pro hodnocení uchazečů, interně vyvinutý proctoring, chatbot napojený na neveřejné studijní spisy nebo vlastní model vyhodnocující riziko studijní neúspěšnosti.

Z hlediska GDPR je škola obvykle správcem osobních údajů žáků a zaměstnanců. Dodavatel AI služby je typicky zpracovatelem, pokud zpracovává údaje podle pokynů školy, nebo samostatným správcem, pokud si určuje vlastní účely zpracování. Tento rozdíl musí být posouzen před zavedením AI systému a promítnut do smluvní dokumentace, informační povinnosti a evidence zpracování.

4. Riziková kategorizace AI ve škole podle AI Act

AI Act pracuje s rizikovým přístupem. Pro školu je klíčové rozlišit běžné podpůrné použití AI, transparentnostní povinnosti, vysoce rizikové vzdělávací systémy a zakázané praktiky. Níže uvedená matice slouží jako interní pomůcka pro prvotní posouzení; nenahrazuje právní, bezpečnostní a datové posouzení konkrétního systému.

Použití AI ve škole	Typické příklady	Předběžné zařazení	Minimální opatření
Obecná generativní AI pro přípravu učitele	Návrh osnovy hodiny, jazyková korektura, shrnutí veřejných zdrojů, tvorba ilustračních příkladů bez osobních údajů.	Zpravidla nižší riziko, avšak s povinností AI gramotnosti, kontroly výstupů a ochrany dat.	Schválený nástroj, zákaz osobních údajů do veřejné AI, odborný přezkum, evidence významného použití.
AI pomůcka pro žáka	Brainstorming, vysvětlení pojmu, procvičovací otázky, překlad, úprava stylu textu.	Zpravidla pedagogické použití s pravidly akademické integrity.	Jasně zadání, co je povoleno; povinnost přiznat AI použití; žádné vydávání AI výstupu za vlastní práci.
Automatizované přijímání a přiřazování	Skórování uchazečů, doporučení přijetí/nepřijetí, přiřazení do programu, skupiny nebo úrovně podle algoritmu.	Vysoce rizikové použití podle AI Act.	Předběžné schválení, DPIA/FRIA, lidské rozhodnutí, transparentnost, audit vstupních dat, možnost odvolání.
Hodnocení výsledků učení	Automatické známkování, generování bodů, adaptivní systém určující postup žáka, AI feedback použitý pro známku.	Vysoce rizikové, pokud systém hodnotí výsledky učení nebo řídí učební proces.	AI nesmí být jediný základ výsledku; učitel kontroluje a dokumentuje přezkum; pravidla pro námitku žáka.
Analýza studijních dat	Predikce rizika neúspěchu, doporučení podpůrných opatření, profil studijních návyků, klasifikace výkonnosti.	Podle účelu může být vysoce rizikové a zároveň profilování podle GDPR.	Minimalizace, vysvětlitelnost, zákaz stigmatizace, lidské posouzení, přístup jen oprávněným osobám.
Monitoring testů a zakázaného chování	AI proctoring, detekce opisování, analýza obrazu, zvuku, pohybu očí nebo aktivity zařízení.	Vysoce rizikové použití; některé biometrické nebo emoční funkce mohou být zakázané.	Použit jen výjimečně, po DPIA/FRIA, s alternativami, transparentností, přezkumem člověkem a bez sole reliance.
Chatbot na webu školy	FAQ k přijímacímu řízení, rozvrhům, administrativním postupům, navigace po webu.	Transparentnostní povinnost; vyšší riziko při personalizaci nebo rozhodování.	Jasně označit AI, omezit na obecné informace, zákaz citlivých údajů, eskalace na člověka, logy a retence.
Kamerová AI a biometrie	Rozpoznávání obličejů, analýza emocí/pozornosti, detekce chování, biometrická docházka.	Vysoké riziko nebo zakázaná praktika podle účelu; vždy zvýšené GDPR riziko.	Běžné CCTV oddělit od AI funkcí; biometrie jen po zvláštním schválení; zákaz detekce emocí ve výuce mimo úzké výjimky.

4.1 Vysoce rizikové systémy ve vzdělávání

Za vysoce rizikové se ve školství považují zejména AI systémy určené k určování přístupu nebo přijetí ke vzdělávání, k přiřazení osob do vzdělávacích institucí nebo programů, k hodnocení výsledků učení, včetně řízení učebního procesu, k posouzení vhodné úrovně vzdělávání a k monitorování nebo detekci zakázaného chování žáků během testů.

Škola nesmí vysoce rizikový AI systém zavést jen na základě marketingového popisu dodavatele. Před zavedením musí ověřit určený účel, právní zařazení, poskytovatele, dostupnost technické dokumentace a pokynů pro použití, možnost lidského dohledu, vedení logů, bezpečnost, kvalitu vstupních dat, nediskriminaci a dopady na práva žáků.

4.2 Zakázané praktiky zvlášť významné pro školu

Ve školním prostředí jsou zvlášť rizikové zejména AI systémy, které manipulují chování žáka, využívají zranitelnost z důvodu věku, zdravotního postižení nebo sociální situace, vytvářejí sociální skóre, skrytě ovlivňují rozhodování, biometricky kategorizují osoby podle citlivých charakteristik nebo vyvozují emoce osob ve vzdělávací instituci mimo úzké zdravotní či bezpečnostní výjimky. Škola takové systémy nesmí pořizovat, aktivovat ani používat.

5. Zásady odpovědného používání AI ve škole

Každé použití AI musí respektovat následující zásady. Tyto zásady se uplatní bez ohledu na to, zda jde o placený školní nástroj, veřejnou službu, doplněk v kancelářském balíku, překladač, chatbot, systém ve studijním informačním systému nebo AI funkci dodavatele.

- **Zákonnost a legitimní účel:** AI lze použít jen pro účel slučitelný s výukou, výzkumem, školní administrativou, bezpečností nebo jinou zákonnou činností školy.
- **Přiměřenost:** AI se nepoužije tam, kde lze účelu dosáhnout méně invazivním nebo pedagogicky vhodnějším postupem.
- **Minimalizace dat:** Do AI se vkládá jen nezbytný rozsah údajů; přednost má anonymizace, agregace nebo pseudonymizace.
- **Lidská odpovědnost:** Za použití AI výstupu odpovídá konkrétní osoba, nikoli systém. AI výstup je návrh nebo podpůrný podklad, ne automatická pravda.
- **Transparentnost:** Žáci a zákonní zástupci musí vědět, kdy AI významně ovlivňuje jejich výuku, hodnocení, komunikaci nebo rozhodnutí školy.
- **Nediskriminace:** AI nesmí znevýhodňovat osoby podle věku, pohlaví, zdravotního stavu, postižení, jazyka, sociální situace, etnicity, náboženství nebo jiných chráněných charakteristik.
- **Bezpečnost a důvěrnost:** AI se používá jen v režimu odpovídajícím povaze dat a v souladu s pravidly kybernetické bezpečnosti.
- **Auditovatelnost:** U významných rozhodnutí musí být dohledatelné, zda byla AI použita, jaká data byla zpracována, kdo provedl lidský přezkum a jak byl výstup zohledněn.

5.1 Pravidlo „žádné osobní údaje do veřejné AI“

Do veřejných AI systémů je zakázáno vkládat jména žáků, rodná čísla, kontaktní údaje, fotografie, nahrávky, individuální výsledky studia, známky, kázeňské záznamy, zdravotní údaje, údaje o podpůrných opatřeních, údaje školního poradenského pracoviště, osobní nebo rodinné okolnosti, přístupové údaje, školní identifikátory nebo dokumenty umožňující identifikaci osoby. Zákaz platí i pro „pouhé vyzkoušení“, rychlou korekturu, překlad nebo anonymizaci, pokud anonymizace není skutečně provedena před vložením.

5.2 Pravidlo „AI nikdy sama nerozhoduje o žákovi“

AI nesmí být jediným nebo rozhodujícím podkladem pro přijetí/nepřijetí ke studiu, známku, vyloučení, kázeňské opatření, přiznání či nepřiznání podpůrných opatření, posouzení plagiátorství, určení studijního plánu, zařazení do skupiny, omezení přístupu ke službě školy nebo jiné rozhodnutí s významným dopadem na žáka. Pokud je AI použita jako podpůrný podklad, musí existovat skutečný lidský přezkum a možnost žáka se vyjádřit.

6. Používání AI nástrojů učitelů, zaměstnanců a žáků

6.1 Používání nástrojů typu ChatGPT, Copilot a obdobných asistentů zaměstnanci

Pedagogičtí a nepedagogičtí zaměstnanci mohou používat schválené AI nástroje pro pracovní účely, pokud tím neporušují ochranu osobních údajů, důvěrnost, autorská práva, pravidla školy a zásady pedagogické odpovědnosti. Typicky je přípustné použít AI pro návrh osnovy hodiny, příkladů, jazykovou korekturu, překlad obecného textu, shrnutí veřejného materiálu, návrh testových otázek bez odpovědí navázaných na konkrétní žáky, podporu tvorby prezentace, technickou pomoc při tabulkách nebo generování administrativního vzoru.

Zaměstnanec nesmí do veřejného AI systému zadat identifikovatelnou žákovskou práci, posudek, známky, záznam z jednání, doporučení pedagogicko-psychologické poradny, zdravotní údaj, fotografie žáků, interní e-mailovou komunikaci s osobními údaji nebo neveřejné dokumenty školy, pokud nástroj nebyl výslovně schválen pro danou kategorii dat a pro daný účel.

Používá-li zaměstnanec nástroj integrovaný do kancelářského balíku nebo školního účtu, například Copilot, musí ověřit, že jde o školou spravovaný účet, schválenou licenci, nastavenou ochranu dat a že AI funkce nemá přístup k souborům nebo e-mailům nad rámec oprávnění uživatele. Zaměstnanec nesmí pro pracovní úkoly používat soukromý placený účet, anonymní účet nebo neschválené rozšíření prohlížeče.

6.2 Překladače a jazykové nástroje

Překladače a jazykové korektory jsou AI nástroje a vztahují se na ně stejná pravidla. Lze je používat pro veřejné nebo anonymizované texty, jazykovou podporu a přípravu materiálů. V jazykové výuce, testech a zkouškách musí učitel v zadání výslovně stanovit, zda jsou překladače povoleny, omezeny nebo zakázány. Pokud je překladač použit v žákem odevzdávané práci, žák musí postupovat podle pravidel zadání a případně použití přiznat.

6.3 Používání AI žáky

Žák může používat AI nástroje k učení, vysvětlení látky, procvičování, překladu, brainstormingu, tvorbě osnovy, kontrole pravopisu nebo technické pomoci, pokud to není v rozporu se zadáním, pravidly předmětu nebo pravidly akademické integrity. Žák vždy odpovídá za odevzdaný obsah, faktickou správnost, uvedené zdroje a přiznání pomoci AI.

Pro každé zadání musí být pokud možno stanoveno, do kterého režimu spadá:

Režim zadání	Význam	Požadavek na žáka
AI zakázána	AI nesmí být použita pro tvorbu řešení, textu, kódu nebo odpovědi. Lze povolit pouze běžné nástroje dostupnosti, pokud je to uvedeno.	Odevzdaná práce musí být výsledkem samostatné práce. Porušení se posuzuje jako porušení akademické integrity.
AI povolena s přiznáním	AI lze použít jako pomocný nástroj, ale žák musí uvést, k čemu a v jakém rozsahu ji použil.	Přiložit prohlášení o použití AI; ověřit výstupy; citovat zdroje; nepřevzít neověřené tvrzení.
AI doporučena nebo vyžadována	AI je součástí výukového cíle, například porovnání výstupů, prompt engineering, kritická analýza nebo automatizace.	Postupovat podle metodiky; dokumentovat prompty nebo výstupy v rozsahu stanoveném učitelem.
AI jako kompenzační nebo podpůrná pomůcka	AI pomáhá s dostupností, překladem, čtením, strukturováním nebo asistenční funkcí.	Použití se řeší individuálně, zejména u podpůrných opatření; nemá vést k nepříměřenému znevýhodnění.

6.4 Zakázané jednání žáků

- odevzdat AI výstup jako vlastní práci, pokud zadání vyžaduje vlastní řešení;
- vytvořit falešné citace, falešné zdroje, falešné laboratorní výsledky, falešná data nebo nepravdivé důkazy;
- použít AI k obcházení technických kontrol, proctoringu, přístupových omezení nebo bezpečnostních pravidel školy;
- vkládat do veřejné AI osobní údaje spolužáků, učitelů, zaměstnanců nebo třetích osob bez právního důvodu;
- generovat deepfake, napodobeniny hlasu nebo obrazu reálných osob, šikanující, ponižující, sexuální, diskriminační nebo manipulační obsah;
- použít AI k neoprávněnému získání odpovědi při testu, zkoušce, soutěži nebo přijímacím řízení.

7. AI ve výuce, domácí přípravě, písemných pracích a hodnocení

7.1 Pedagogické použití AI

Pedagogické použití AI musí podporovat vzdělávací cíle, nikoli nahrazovat odbornou a pedagogickou odpovědnost učitele. Učitel smí použít AI například k návrhu variant úkolů, diferenciaci obtížnosti, tvorbě cvičení, podpoře čtenářské srozumitelnosti, přípravě příkladů pro žáky s různou úrovní znalostí nebo pro dostupnost materiálů. Každý takový výstup musí učitel před použitím ověřit, upravit a posoudit vhodnost pro věk, schopnosti a kontext žáků.

Při tvorbě učebních materiálů je třeba ověřit zejména věcnou správnost, aktuálnost, zdroje, možné předsudky, přiměřenost věku, jazykovou kulturu, absenci diskriminačních stereotypů a právní použitelnost

obrázků, příkladů, testů a datových sad. AI výstup nesmí být použit jako náhrada odborné přípravy učitele nebo jako zdroj faktů bez kontroly.

7.2 AI v hodnocení

Použití AI v hodnocení je vysoce citlivé. AI může pomoci s návrhem hodnoticí rubriky, s formální kontrolou nebo s přípravou zpětné vazby, ale finální hodnocení provádí učitel nebo komise. Pokud AI výstup ovlivní bodové nebo slovní hodnocení, musí být doložitelné, kdo AI použil, jaký byl účel, jak byl výstup přezkoumán a jaká část výsledku je lidským rozhodnutím.

AI nesmí automaticky určovat známku, přijetí, neúspěch, kázeňské opatření ani závěr o podvodu. U písemných prací, kódů, projektů a zkoušek je možné použít AI jako podpůrný nástroj pro kontrolu konzistence nebo formálních znaků, nikoli jako jediný důkaz. Žák musí mít možnost seznámit se s podstatou výhrad, vyjádřit se k nim a navrhnout vysvětlení nebo důkazy.

7.3 AI detektory a akademická integrita

AI detektory jsou nespolehlivé jako samostatný důkaz a mohou vykazovat falešně pozitivní i falešně negativní výsledky. Jejich použití je možné pouze jako jeden z podpůrných signálů, pokud je systém schválen, je posouzena ochrana osobních údajů a žáci byli předem informováni. Detektor nesmí nahradit pedagogické posouzení, ústní obhajobu, srovnání s předchozími pracemi, analýzu verzí dokumentu, posouzení citací a další přiměřené postupy.

Podezření na nepovolené použití AI se řeší postupem, který chrání práva žáka. Minimálně musí být zaznamenán důvod podezření, použitý nástroj, výsledek a jeho omezení, další zjištěné skutečnosti, vyjádření žáka, závěr učitele nebo komise a možnost přezkumu podle vnitřních pravidel školy.

8. Automatizované systémy, studijní systémy, hodnocení a analýzy dat

Studijní informační systém, LMS, elektronická žákovská knížka, rozvrhový systém, knihovní systém, systém pro přijímací řízení nebo datový sklad sám o sobě nemusí být AI systémem. AI režim se však aktivuje, pokud systém začne generovat predikce, doporučení, klasifikace, automatické závěry, profilování nebo rozhodnutí s určitou mírou autonomie.

8.1 Příklady automatizace a požadovaný režim

Funkce systému	Příklad	Riziko	Požadovaný postup
Administrativní automatizace	Automatické připomenutí termínu, řazení přihlášek podle data, export dat.	Nízké až střední, pokud nejde o hodnocení osob.	Běžné ICT schválení, ochrana dat, kontrola správnosti.
Doporučovací systém ve výuce	LMS doporučí procvičování podle výsledků testů.	Střední až vysoké, pokud řídí učební cestu nebo ovlivňuje hodnocení.	Pedagogický dohled, informování žáků, možnost alternativy a kontrola dopadů.
Predikce rizika neúspěchu	Systém označí žáka jako rizikového podle docházky, známek a aktivity.	Profilování, riziko stigmatizace a diskriminace.	DPIA, minimalizace dat, poradenský lidský přezkum, zákaz automatických sankcí.
Přijímací scoring	Algoritmus doporučí přijetí/nepřijetí nebo pořadí uchazečů.	Vysoce rizikové.	DPIA/FRIA, právní schválení, lidská komise, audit dat, transparentnost uchazečům.
Automatické hodnocení	AI opravuje esej, kód, odpovědi nebo generuje body.	Vysoce rizikové při hodnocení výsledků učení.	Učitel odpovídá za výsledek; AI jen podpůrně; dokumentace a námitkový mechanismus.
Proctoring	AI sleduje obraz, zvuk, pohyb očí nebo obrazovku při testu.	Vysoce rizikové, často velmi invazivní.	Výjimečné použití, DPIA/FRIA, alternativy, transparentnost, omezení retence, lidské posouzení.

8.2 Zásady pro analýzu studijních dat

- Analytika nesmí vytvářet trvalé „nálepky“ žáků, například „rizikový“, „slabý“, „neperspektivní“, bez kontextu, pedagogického přezkumu a možnosti změny.
- Predikce rizika neúspěchu slouží pouze k nabídce podpory, nikoli k sankci, vyloučení, omezení příležitostí nebo snížení očekávání.
- Do modelů se nesmí bez zvláštního schválení zahrnovat citlivé údaje, zdravotní údaje, údaje o podpůrných opatřeních, sociální situaci, rodinných poměrech nebo disciplinární záznamy.

- Pokud je analytika založena na historických datech, musí být posouzeno riziko reprodukce minulých nerovností a proxy proměnných.
- Výstupy musí být srozumitelné pedagogům, žákům i osobám provádějícím dohled; neprůhledný model bez možnosti vysvětlit důvod doporučení není vhodný pro zásadní školská rozhodnutí.

8.3 Minimální dokumentace automatizovaného systému

U každého systému, který provádí hodnocení, predikci, doporučení nebo klasifikaci žáků, se vede dokumentace obsahující alespoň název systému, dodavatele, vlastníka procesu, účel, popis AI funkce, právní základ zpracování, kategorie dat, dotčené osoby, typ výstupu, vliv na rozhodnutí, opatření lidského dohledu, výsledky testování, záznam o schválení, dobu retence, seznam oprávněných osob a datum příští revize.

9. Chatbot na webu školy a AI v komunikaci se žáky a rodiči

Chatbot na webu školy může významně zlepšit dostupnost obecných informací, ale současně přináší riziko nesprávných odpovědí, nechtěného sběru osobních údajů, mylného dojmu závazného rozhodnutí školy a bezpečnostních útoků typu prompt injection. Chatbot proto smí být nasazen pouze jako schválený AI systém s jasně vymezeným účelem, znalostní bází, odpovědnou osobou, informační povinností a mechanismem předání na člověka.

9.1 Povolené a zakázané použití chatbotu

Povolené použití	Nepřípustné bez zvláštního schválení
Obecné informace o termínech, přijímacím řízení, kontaktech, úředních hodinách, rozvrhových pokynech, navigaci po webu, školním řádu a veřejných dokumentech.	Individuální právně nebo studijně závazné rozhodování o přijetí, uznání předmětů, klasifikaci, kázeňském opatření, nároku na podporu nebo zdravotních a poradenských otázkách.
Odkazování na oficiální zdroje školy a předání kontaktu na studijní oddělení, třídního učitele, sekretariát, DPO nebo IT podporu.	Přístup chatbotu do neveřejných studijních spisů, známek, zdravotních záznamů, poradenské dokumentace nebo e-mailů bez výslovného schválení a posouzení dopadů.
Sběr obecné zpětné vazby, pokud je anonymní nebo přiměřeně informovaný.	Skryté profilování návštěvníků webu, sledování chování žáků, cílení sdělení podle citlivých znaků nebo manipulativní komunikace.

9.2 Transparentnost chatbotu

Chatbot musí být zřetelně označen tak, aby uživatel před zahájením komunikace věděl, že komunikuje s AI systémem. Oznámení musí být viditelné, srozumitelné a doplněné o upozornění, že chatbot poskytuje pouze obecné informační odpovědi a závazné informace nebo rozhodnutí poskytuje výhradně oprávněná osoba školy.

Doporučené úvodní oznámení: „Komunikujete s AI chatbotem školy. Chatbot poskytuje pouze obecné informace z veřejných zdrojů školy. Nezadávejte prosím citlivé nebo osobní údaje, které nejsou nezbytné. Pokud potřebujete individuální, závazné nebo citlivé řešení, kontaktujte příslušné pracoviště školy.“

9.3 Provozní a bezpečnostní požadavky

- Chatbot musí používat schválenou a pravidelně aktualizovanou znalostní bázi; odpovědi bez opory ve zdroji mají být omezeny nebo označeny jako nejisté.
- Musí být nastaveny hranice témat, odmítnutí odpovědi a předání na člověka pro individuální studijní, právní, zdravotní, psychologické nebo bezpečnostní otázky.
- Logy konverzací se uchovávají jen po přiměřenou dobu a v rozsahu nezbytném pro bezpečnost, kvalitu a řešení incidentů.
- Chatbot nesmí poskytovat interní instrukce, systémové prompty, neveřejné dokumenty, osobní údaje ani údaje získané z jiné konverzace.
- Před spuštěním a pravidelně poté se testují rizikové scénáře, zejména halucinace, nesprávné informace o termínech, prompt injection, žádosti o osobní údaje a odpovědi vůči nezletilým.

10. Kamerové, přístupové, dohledové a biometrické systémy

Běžný kamerový systém, čipový vstup, školní karta nebo evidence přístupů nemusí být AI systémem, pokud pouze zaznamenává obraz nebo umožňuje vstup bez autonomní analýzy. Jakmile je však doplněn o rozpoznávání obličejů, identifikaci osob, detekci emocí, sledování pozornosti, predikci chování, detekci konfliktů nebo jiné automatizované vyvozování závěrů o osobách, musí být posouzen jako AI systém a zpravidla jako použití se zvýšeným nebo vysokým rizikem.

10.1 Zákaz detekce emocí a citlivé biometrické kategorizace

Škola nesmí používat AI systém k vyvozování emocí žáků, učitelů nebo jiných osob ve vzdělávací instituci, například detekci stresu, pozornosti, znučení, únavy, strachu nebo zájmu z obličeje, hlasu, pohybu nebo biometrických znaků, ledaže by šlo o úzce vymezený zákonný zdravotní nebo bezpečnostní důvod a systém prošel zvláštním právním posouzením. Obdobně je zakázána biometrická kategorizace osob za účelem dedukce citlivých charakteristik, například etnicity, politických názorů, náboženství, zdravotního stavu, sexuální orientace nebo obdobných znaků.

10.2 Rozpoznávání obličejů a biometrická docházka

Rozpoznávání obličejů, biometrická docházka, biometrické přístupové systémy nebo identifikace žáků na dálku představují zpracování biometrických údajů a vyžadují mimořádně přísné posouzení nezbytnosti, zákonného důvodu, proporcionality, alternativ, bezpečnosti a práv dotčených osob. Takové systémy nesmí být zavedeny z důvodu pohodlí nebo administrativní úspory, pokud existuje méně invazivní alternativa, například karta, čip, kód nebo ruční ověření.

10.3 AI proctoring a dohled při zkouškách

AI proctoring nebo dohled nad testy je použití s vysokým dopadem na práva žáků. Pokud škola uvažuje o takovém systému, musí předem doložit legitimní účel, nezbytnost, absenci méně invazivní alternativy, přesnost, omezení falešných pozitiv, práva žáků se zdravotním postižením nebo zvláštními potřebami, pravidla lidského přezkumu, retenci záznamů, bezpečnost a možnost alternativního způsobu zkoušky. Pouhý výstup proctoringu nesmí být důvodem sankce bez dalšího posouzení.

10.4 Kamerová analytika v prostorách školy

AI kamerová analytika v prostorách školy, například detekce pohybu, shlukování, konfliktů, podezřelého chování nebo identifikace osob, se smí použít pouze po samostatném schválení. Musí být oddělena od běžného kamerového systému, jasně popsána v informačním oznámení, omezena na nezbytné prostory a účely a nesmí vést k plošnému sledování žáků nebo zaměstnanců. U nezletilých osob je nutné posuzovat zásah do soukromí zvlášť přísně.

11. Práce s osobními údaji žáků, uchazečů, rodičů a zaměstnanců

AI systémy mohou zpracovávat osobní údaje pouze tehdy, je-li to zákonné, nezbytné, přiměřené a schválené pro daný účel. Ve školství se osobní údaje často týkají nezletilých, vzdělávacích výsledků, sociální situace, zdravotního stavu, podpůrných opatření nebo poradenských informací, a proto je nutné uplatnit zvýšený režim ochrany.

11.1 Kategorie údajů se zvýšenou ochranou

Kategorie údajů	Příklady	Pravidlo pro AI
Identifikační a kontaktní údaje	Jméno, e-mail, telefon, adresa, ID žáka, třída, ročník.	Do veřejné AI zakázáno; ve schválené AI jen pokud je nezbytné a smluvně zajištěné.
Studijní údaje	Známky, docházka, výsledky testů, práce žáků, plány studia.	Použití pro analýzu nebo hodnocení vyžaduje posouzení účelu, minimalizace a lidský dohled.
Kázeňské a behaviorální údaje	Napomenutí, záznamy incidentů, chování při testu, proctoring.	Vysoké riziko; nepoužívat pro profilování bez právního posouzení a námitkového mechanismu.
Zdravotní a poradenské údaje	Podpůrná opatření, diagnózy, zdravotní omezení, zprávy poradny.	Zvláštní kategorie údajů; do veřejné AI zakázáno; ve schválené AI jen výjimečně a po DPIA.
Obrazové a zvukové záznamy	Fotografie, video z výuky, online zkoušky, nahrávky hlasu.	Použití pro AI analýzu jen po zvláštním schválení; biometrické a emoční funkce zásadně nepřipustné.

Údaje zákonných zástupců	Kontakty rodičů, komunikace se školou, rodinné okolnosti.	Minimalizovat; nepoužívat pro profilování žáka nebo rodiny bez výslovného právního důvodu.
---------------------------------	---	--

11.2 Právní základy a souhlas

Právní základ zpracování osobních údajů v AI systémech se stanoví podle konkrétního účelu. Ve veřejném školství půjde často o splnění právní povinnosti nebo úkol ve veřejném zájmu; u některých podpůrných služeb o smluvní vztah nebo oprávněný zájem; souhlas se použije pouze tehdy, pokud je skutečně svobodný, konkrétní, informovaný a odvolatelný. Souhlas žáka nebo rodiče není vhodný pro zpracování, které je fakticky povinné nebo kde je žák ve vztahu závislosti na škole.

11.3 DPIA, FRIA a posouzení dopadů

Před zavedením AI systému, který systematicky hodnotí žáky, zpracovává rozsáhlé studijní údaje, provádí profilování, používá biometrická data, analyzuje obraz nebo zvuk, používá citlivé údaje nebo může významně ovlivnit práva žáků, škola provede posouzení dopadů na ochranu osobních údajů (DPIA). U vysoce rizikových AI systémů používaných veřejnoprávní školou nebo školou poskytující veřejnou službu se současně posoudí dopad na základní práva (FRIA) v rozsahu vyžadovaném AI Act.

DPIA a FRIA mohou být prakticky spojeny do jednoho procesu, ale musí pokrýt oba okruhy: ochranu osobních údajů a širší základní práva, například právo na vzdělání, nediskriminaci, spravedlivý proces, ochranu dítěte, svobodu projevu, lidskou důstojnost a přístupnost pro osoby se zdravotním postižením.

11.4 Zákaz používání vstupů pro trénink mimo kontrolu školy

Škola nesmí schválit AI systém pro zpracování osobních nebo důvěrných údajů, pokud dodavatel používá vstupy, výstupy nebo metadata školy pro další trénink nebo zlepšování modelů bez jasného právního důvodu, smluvní kontroly a možnosti odmítnutí. Smlouva musí upravit účely zpracování, subdodavatele, místa zpracování, předávání mimo EHP, dobu uchování, mazání, audit, incidenty, asistenci při právech subjektů údajů a ukončení služby.

12. Interní správa AI, schvalování, evidence a odpovědnosti

Škola vede centralizovanou evidenci AI systémů a AI funkcí používaných pro školní účely. Bez evidence a schválení nesmí být AI systém použit pro zpracování osobních údajů, hodnocení žáků, přijímací řízení, bezpečnostní dohled, chatbot, integraci do studijního systému ani jiný účel s dopadem na žáky.

12.1 Schvalovací proces

1. Vlastník procesu popíše účel, očekávaný přínos, dotčené osoby, typ výstupu, datové kategorie a zamýšlené použití AI.
2. ICT nebo bezpečnostní správce posoudí architekturu, účty, přístupy, logování, šifrování, integrace, exporty, dostupnost a incident response.
3. DPO posoudí osobní údaje, právní základ, informační povinnost, práva subjektů údajů, DPIA a předávání údajů.
4. Právní nebo compliance role posoudí AI Act zařazení, smlouvy, autorská práva, odpovědnost, školské předpisy a vynutitelnost pravidel.
5. Pedagogický garant posoudí vhodnost pro výuku, věk žáků, přístupnost, dopady na rovnost a metodiku použití.
6. Vedení školy rozhodne o schválení, podmínkách, pilotním provozu, zákazu nebo dalším posouzení.

12.2 Evidence AI systému

Evidovaný údaj	Minimální obsah
Název a dodavatel	Název systému, verze, poskytovatel, smluvní partner, kontaktní osoba.
Účel a určený účel	K čemu systém smí být použit; zakázané nebo neschválené účely.
AI Act zařazení	Nízké / transparentnostní / vysoce rizikové / zakázané / mimo AI Act; odůvodnění.
Dotčené osoby	žáci, zákonní zástupci, zaměstnanci, veřejnost, dodavatelé.

Data a zdroje dat	Kategorie údajů, zdroj, rozsah, citlivé údaje, vstupní dokumenty, retence.
Vliv na rozhodnutí	Zda je výstup informativní, doporučující, hodnotící nebo rozhodovací.
Lidský dohled	Kdo výstup kontroluje, kdy může zasáhnout, jak se dokumentuje odchylka.
Schválení a revize	Datum schválení, schvalující osoba, podmínky, datum příští revize, pilotní režim.

12.3 Vymezení odpovědnosti

Role	Hlavní odpovědnost
Ředitel / vedení školy	Schvaluje směrnici, vymezuje odpovědnosti, rozhoduje o systémech s vysokým dopadem a zajišťuje zdroje pro compliance.
Vlastník procesu	Nese odpovědnost za věcný účel AI, přiměřenost použití, dokumentaci procesu a splnění podmínek schválení.
Pedagogický pracovník	Odpovídá za didaktické použití AI, kontrolu výstupů, pravidla zadání, hodnocení a komunikaci se žáky.
Žák	Odpovídá za dodržení zadání, přiznání AI pomoci, pravdivost práce a ochranu údajů třetích osob.
DPO	Posuzuje ochranu osobních údajů, DPIA, informační povinnost, smlouvy o zpracování a práva subjektů údajů.
ICT / bezpečnost	Posuzuje technické zabezpečení, účty, integrace, logy, přístupy, incidenty a provozní bezpečnost.
Právní / compliance	Posuzuje AI Act, smluvní rámec, odpovědnost, autorská práva, školské předpisy a zakázané praktiky.
Dodavatel	Plní smluvní, bezpečnostní, dokumentační a zpracovatelské povinnosti; poskytuje pokyny pro použití a součinnost škole.

12.4 Nákup a smluvní požadavky

- Dodavatel musí popsat, zda jde o AI systém, jaký je jeho určený účel, jaké výstupy generuje a jaká jsou známá omezení.
- U vysoce rizikového systému musí být k dispozici dokumentace, pokyny pro použití, informace pro lidský dohled, evidence shody, logování a součinnost s DPIA/FRIA.
- Smlouva musí obsahovat zpracovatelskou smlouvu nebo jiné odpovídající ujednání, zákaz nepovoleného tréninku na datech školy, pravidla retence, subdodavatele, bezpečnost, incidenty, audit a exit plán.
- Dodavatel nesmí jednostranně aktivovat nové AI funkce s dopadem na data nebo žáky bez předchozího oznámení a schválení školy.
- U cloudových služeb se posoudí umístění dat, předávání mimo EHP, šifrování, správa klíčů, logy, SSO/MFA a možnost exportu a výmazu dat.

13. Transparentnost vůči žákům, rodičům a ochrana práv žáků

Transparentnost je základní podmínkou důvěryhodného použití AI ve škole. Žák nebo zákonný zástupce musí být srozumitelně informován, pokud AI významně vstupuje do výuky, hodnocení, přijímacího řízení, komunikace, dohledu, bezpečnosti nebo zpracování osobních údajů. Informace musí být přiměřená věku, roli a situaci dotčené osoby.

13.1 Minimální obsah informační povinnosti

- že je používán AI systém a jaký je jeho název nebo kategorie;
- účel použití a zda AI pouze pomáhá člověku, nebo významně ovlivňuje výsledek;
- jaké osobní údaje nebo školní údaje jsou zpracovávány a z jakých zdrojů;
- zda jde o vysoce rizikové použití, hodnocení, profilování nebo automatizovaný podklad;
- kdo je odpovědná osoba školy a kdo provádí lidský dohled;
- jak lze požádat o vysvětlení, opravu, lidský přezkum nebo podat námitku/stížnost;
- doba uchování údajů, hlavní příjemci a informace o dodavateli, pokud je relevantní;
- zda existuje alternativní postup, zejména u proctoringu, biometrie, accessibility nástrojů nebo citlivých situací.

13.2 Práva žáků

Žák má právo nebýt vystaven významnému rozhodnutí školy založenému výhradně na AI výstupu, pokud právní předpisy neumožňují jinak a nejsou zajištěny odpovídající záruky. Žák má právo na lidský přezkum, možnost vyjádření, opravu zjevně chybných údajů, vysvětlení podstatných důvodů rozhodnutí a přiměřenou námitku nebo opravný prostředek podle vnitřních a právních pravidel školy.

U nezletilých žáků musí být informace poskytována také zákonným zástupcům, pokud to odpovídá povaze zpracování, věku žáka a právnímu režimu. Informace pro mladší žáky musí být formulována jednoduše a srozumitelně, nikoli jen právním textem.

13.3 Ochrana zranitelných skupin a přístupnost

AI systém nesmí žáky znevýhodňovat z důvodu zdravotního postižení, neurodiverzity, jazyka, sociální situace, věku, pohlaví nebo jiných charakteristik. Před nasazením AI ve výuce, hodnocení nebo dohledu se posoudí dostupnost pro žáky se speciálními vzdělávacími potřebami, možnost lidské podpory, alternativního plnění a riziko nepřiměřené zátěže.

14. Zakázané způsoby použití AI a zvláštní omezení ve školství

Je zakázáno používat AI způsobem, který je v rozporu s právními předpisy, školními předpisy, dobrými mravy, profesní etikou, pravidly akademické integrity nebo touto směrnicí. Následující zákazy platí pro zaměstnance, žáky i dodavatele v rozsahu jejich role.

- používat AI k manipulaci žáků, skrytému ovlivňování jejich rozhodnutí nebo využívání zranitelnosti z důvodu věku, postižení nebo sociální situace;
- používat AI k sociálnímu skórování žáků, rodin nebo zaměstnanců;
- používat AI k vyvozování emocí ve vzdělávací instituci, například pozornosti, stresu nebo zájmu, mimo úzce zákonné zdravotní nebo bezpečnostní výjimky;
- používat biometrickou kategorizaci k odvozování citlivých charakteristik;
- vytvářet nebo šířit deepfake, napodobeniny hlasu, nepravdivé důkazy, falešné citace, falešné posudky nebo klamavá sdělení;
- nahrávat do neschválené AI databáze žáků, třídní seznamy, studijní spisy, zdravotní nebo poradenskou dokumentaci, záznamy z kamer či online výuky;
- používat AI jako jediný důkaz akademického podvodu, jediný podklad známky nebo jediný podklad rozhodnutí o přijetí či vyloučení;
- aktivovat AI doplňky v LMS, kancelářském balíku, prohlížeči, e-mailu, úložišti nebo studijním systému bez schválení;
- předávat AI systému přístupové údaje, API klíče, hesla, neveřejné bezpečnostní konfigurace nebo zranitelnosti školy bez bezpečnostního režimu;
- používat AI k neoprávněnému monitorování zaměstnanců, žáků nebo zákonných zástupců.

15. Pravidla kontroly používání AI a akademické integrity

Škola je oprávněna přiměřeně, transparentně a dokumentovaně kontrolovat, zda jsou AI systémy používány v souladu s touto směrnicí, školním řádem, pravidly akademické integrity a požadavky na ochranu dat. Kontrola musí být vždy nezbytná, přiměřená a musí respektovat lidskou důstojnost, soukromí, práva ýáků a pracovněprávní pravidla.

15.1 Kontrola zaměstnanců

U zaměstnanců může kontrola zahrnovat přehled schválených aplikací, licence, účty, auditní logy, nastavení sdílení, typy nahraných souborů, metadata použití a bezpečnostní konfigurace. Obsah promptů, dokumentů nebo konverzací lze kontrolovat jen tehdy, je-li to nezbytné pro řešení konkrétního podezření,

incidentu, zákonné povinnosti nebo ochranu důležitých práv školy či třetích osob. Přednost mají méně invazivní prostředky.

15.2 Kontrola žáků a podezření na nepovolené použití AI

Kontrola žákovských prací musí být předvídatelná. Žák má být předem informován, jaké nástroje a postupy mohou být použity k ověření originality, plagiátorství nebo nepovoleného použití AI. Výsledky automatizovaných nástrojů jsou podpůrné a musí být doplněny lidským posouzením. Při podezření musí být žákovi sděleny podstatné důvody a musí dostat přiměřenou možnost vyjádření.

15.3 Dokumentace kontroly

O kontrole se vede záznam obsahující důvod, předmět, rozsah, kontrolující osoby, použitý nástroj, zjištění, vyjádření dotčené osoby, závěr a nápravná opatření. Vzor záznamu je uveden v příloze. Záznam nesmí obsahovat nadbytečné osobní údaje ani celé práce nebo konverzace, pokud postačuje odkaz nebo výňatek nezbytný pro posouzení.

16. Požadavky na ochranu osobních údajů a informační bezpečnost u AI systémů

Každý AI systém určený pro školní použití musí před zavedením projít přiměřeným právním, bezpečnostním, pedagogickým a provozním posouzením. Rozsah posouzení odpovídá rizikovosti použití, kategoriím dat, dotčeným osobám, integračnímu modelu, dodavatelskému řetězci, schopnostem systému a možným dopadům na práva žáků nebo bezpečnost školy.

16.1 Minimální schvalovací kritéria

Oblast	Co musí být posouzeno	Minimální výstup	Odpovědnost
AI Act a školské právo	AI Act role, riziková kategorie, vysoce rizikové použití, zakázané praktiky, dopad na hodnocení a právo na vzdělání.	Právní zařazení a podmínky použití.	Compliance / právní / DPO / vedení školy
Ochrana osobních údajů	Právní základ, kategorie údajů, děti a žáci, minimalizace, DPIA, informační povinnost, práva subjektů, předávání mimo EHP.	Záznam o posouzení, DPIA podle potřeby, informační text.	DPO / vlastník procesu
Základní práva	Nediskriminace, dostupnost, dopad na vzdělání, možnost obrany, lidský dohled, riziko stigmatizace.	FRISA nebo zjednodušené posouzení dopadů.	Vedení / DPO / pedagogický garant
Bezpečnost	SSO, MFA, role, šifrování, logování, integrace, API, export, mazání, zálohy, incident response.	Bezpečnostní akceptace a nastavení.	ICT / bezpečnost
Dodavatel a smlouva	DPA, zákaz tréninku na datech školy, subdodavatelé, SLA, audit, změny podmínek, exit plán.	Smluvní schválení a provozní podmínky.	Nákup / právní / ICT / DPO
Pedagogika	Vhodnost pro věk, učební cíle, přístupnost, dopad na roli učitele a pravidla hodnocení.	Metodika použití a školení uživatelů.	Pedagogický garant / vedení

16.2 Provozní povinnosti

- pravidelně revidovat oprávnění, účty a skutečné používání AI systému;
- sledovat změny funkcí, obchodních podmínek, subdodavatelů a možností tréninku na datech;
- testovat kvalitu výstupů, přesnost, robustnost, halucinace, zkreslení a bezpečnostní zranitelnosti;
- uchovávat automaticky generované logy u vysoce rizikových systémů nejméně po dobu odpovídající účelu a minimálně v rozsahu vyžadovaném AI Act, není-li zvláštní právní důvod pro jinou dobu;
- vyhodnocovat incidenty, stížnosti, chybné výstupy, diskriminační dopady a nápravná opatření;
- dokumentovat významné změny účelu, datových vstupů, modelu, integrací nebo okruhu uživatelů;
- zajistit proces ukončení služby, exportu a výmazu dat.

16.3 Bezpečnostní minimum pro AI nástroje

- preferovat podnikové nebo školní licence se správou účtů, SSO, MFA a administrátorskou kontrolou;
- zakázat použití vstupů a výstupů školy pro trénink modelů, pokud není výslovně schváleno;
- omezit sdílení, veřejné publikování, pluginy, konektory a přístup do úložišť podle principu need-to-know;

- nastavit klasifikaci informací a technické bariéry proti vložení zakázaných kategorií dat;
- zajistit logování, detekci neobvyklého použití, správu API klíčů a revizi oprávnění;
- mít postup pro hlášení bezpečnostního incidentu, úniku osobních údajů, chybného AI rozhodnutí nebo podezření na diskriminační výstup.

17. Vlastnictví obsahu, autorská práva, citace a označování AI výstupů

Použití AI při tvorbě materiálů nezavazuje uživatele odpovědnosti za výsledek. Učitel, zaměstnanec nebo žák musí ověřit, zda použití AI výstupu neporušuje autorská práva, databázová práva, práva k osobnosti, důvěrnost, smluvní omezení, pravidla školy nebo práva třetích osob. AI výstup může obsahovat nepřesnosti, podobnost s cizím dílem, nepravdivé citace nebo licenčně problematické prvky.

17.1 Výukové materiály

Materiály vytvořené zaměstnancem v rámci pracovních úkolů s využitím AI se považují za pracovní výstup ve prospěch školy v rozsahu vyplývajícím z právních předpisů, pracovních smluv a interních pravidel. Pokud je významná část materiálu vytvořena AI, má být v interní verzi zaznamenáno, jaký nástroj byl použit, za jakým účelem a kdo provedl odborný přezkum.

17.2 Žákovské práce a přiznání použití AI

Žák musí použití AI přiznat, pokud to vyžaduje zadání, pravidla předmětu nebo pokud AI významně ovlivnila obsah, strukturu, argumentaci, kód, překlad nebo výsledný výstup. Přiznání AI nenahrazuje citování odborných zdrojů. AI sama není spolehlivým zdrojem faktů; tvrzení převzatá nebo inspirovaná AI musí být ověřena z relevantních zdrojů.

Doporučená formulace prohlášení: „Při zpracování této práce jsem použil/a nástroj [název] k účelu [např. brainstorming, jazyková korektura, návrh osnovy, vysvětlení pojmu]. Výstupy jsem ověřil/a a finální text, argumentace a odpovědnost za práci jsou moje. AI nebyla použita způsobem zakázaným zadáním.“

17.3 Označování syntetického obsahu

Pokud škola nebo žák publikuje syntetický obraz, audio, video, deepfake nebo jiný obsah, který může působit jako reálná osoba, událost nebo výrok, musí být obsah zřetelně označen jako vytvořený nebo upravený AI, ledaže je z kontextu zjevné, že jde o ilustraci, satiru, uměleckou tvorbu nebo cvičení a nejsou dotčena práva osob. U reálných osob, žáků a zaměstnanců se vyžaduje zvláštní opatrnost a právní důvod.

18. AI gramotnost, školení a metodická podpora

Škola zajistí přiměřenou úroveň AI gramotnosti osob, které AI systémy používají, spravují, schvalují nebo jejich výstupy zohledňují. AI gramotnost zahrnuje základní pochopení toho, co AI je, jaké nástroje škola používá, jaké jsou jejich přínosy a limity, jak rozpoznat rizika, jak chránit osobní údaje a jak zajistit lidský dohled a práva žáků.

18.1 Povinné okruhy školení zaměstnanců

- právní rámec AI Act, GDPR a školských pravidel;
- schválené a neschválené AI nástroje školy;
- zákaz osobních a citlivých údajů ve veřejné AI;
- riziko halucinací, bias, neaktuálnosti a falešných citací;
- pravidla AI ve výuce, hodnocení a akademické integritě;
- transparentnost vůči žákům a rodičům;
- postup při podezření na nepovolené použití AI žákem;
- incidenty, úniky dat a hlášení podezřelého chování AI systému.

18.2 Role-based školení

Skupina	Rozšířený obsah školení
Vedení školy	AI governance, schvalování, odpovědnosti, rizikové rozhodování, veřejná komunikace a incidenty.
Pedagogové	Didaktické použití AI, pravidla zadání, hodnocení, práce s AI detektory, ochrana žáků a přístupnost.
Studijní / administrativní pracovníci	AI ve studijních systémech, osobní údaje, komunikace, chatbot, uchazeči a informační povinnost.
ICT a bezpečnost	Architektura AI služeb, identity, logy, integrace, API, bezpečnostní testování, incident response a správa dodavatelů.
DPO / právní / compliance	AI Act klasifikace, DPIA/FRIA, smlouvy, transparentnost, práva subjektů, zakázané praktiky a audit.
Žáci	Základy AI gramotnosti, povolené a zakázané použití, citace, kritické ověřování a ochrana osobních údajů.

18.3 Evidence školení

Škola vede evidenci školení zaměstnanců a u vybraných rolí může absolvování školení podmínit přístupem k AI systému. U žáků se AI gramotnost realizuje přiměřeně formou úvodního poučení, pravidel předmětu, metodických materiálů, školního řádu a výuky digitálních kompetencí.

19. Incidenty, stížnosti, nápravná opatření a revize směrnice

19.1 Incidenty

Incidentem souvisejícím s AI je zejména neoprávněné vložení osobních údajů do veřejné AI, únik nebo ztráta dat, chybné či diskriminační AI doporučení použité ve vztahu ke žákovi, neoprávněná aktivace AI funkce, selhání lidského dohledu, použití zakázané biometrické nebo emoční analytiky, bezpečnostní zranitelnost chatbotu, prompt injection, nepravdivá závazná odpověď chatbotu nebo podezření na neoprávněné automatizované rozhodování.

Incident se hlásí bez zbytečného odkladu vlastníkovému systému, ICT bezpečnosti, DPO a vedení školy podle povahy incidentu. Pokud incident zahrnuje osobní údaje, postupuje se podle pravidel pro porušení zabezpečení osobních údajů. Pokud má incident dopad na žáka, škola zajistí přiměřenou nápravu, vysvětlení, lidský přezkum a prevenci opakování.

19.2 Stížnosti a námitky

Žák, zákonný zástupce nebo zaměstnanec může podat stížnost nebo námitku proti použití AI, pokud se domnívá, že AI ovlivnila jeho práva, hodnocení, přístup ke vzdělání, soukromí nebo rovné zacházení. Škola stanoví kontaktní místo a lhůty pro vyřízení. Stížnost se posoudí věcně a nesmí být odmítnuta jen proto, že systém je dodavatelský nebo technicky složitý.

19.3 Revize směrnice

Tato směrnice se přezkoumává nejméně jednou ročně a dále vždy při významné změně AI Act, výkladů Evropské komise nebo národních orgánů, při zavedení nového AI systému s dopadem na žáky, při změně školského procesu, po závažném incidentu nebo při zjištění systematického nesouladu. Revize se provádí ve spolupráci vedení školy, DPO, ICT, pedagogických garantů a dalších vlastníků procesů.

Příloha č. 1: OnePager – 12 pravidel bezpečného a odpovědného používání AI ve škole

- Používej pouze schválené AI nástroje a školou spravované účty.
- Do veřejné AI nekládej osobní údaje žáků, rodičů ani zaměstnanců.
- AI výstup vždy odborně ověř; AI může halucinovat, chybovat nebo vytvářet nepravdivé citace.
- AI nesmí sama rozhodnout o přijetí, známce, kázeňském opatření nebo podvodu.
- Žákům vždy řekni, zda a jak smí AI použít v konkrétním zadání.
- Podezření na AI podvod neřeš pouze AI detektorem; vždy proveď lidské posouzení a dej žákovi možnost vyjádření.
- Chatbot musí být označen jako AI a nesmí poskytovat závazná individuální rozhodnutí.
- Kamerovou AI, rozpoznávání obličejů, proctoring nebo biometrické systémy nepoužívej bez zvláštního schválení.
- Nepoužívej AI k detekci emocí, sociálnímu skórování, manipulaci nebo skrytému sledování.
- U vysoce rizikových systémů zajisti DPIA/FRIA, lidský dohled, logy a možnost obrany žáka.
- Při tvorbě materiálů respektuj autorská práva, důvěrnost a označuj významné syntetické výstupy.
- Každý incident, únik dat nebo podezřelé chování AI nahlas bez zbytečného odkladu.

Příloha č. 2: Quick Guide pro každodenní rozhodování

ANO – zpravidla přípustné	NE – bez schválení zakázané
Navrhnout osnovu hodiny, pracovní list, cvičení nebo varianty vysvětlení látky bez osobních údajů.	Vložit do veřejné AI práci konkrétního žáka, známky, zdravotní údaje, poradenskou zprávu nebo třídní seznam.
Použít AI překlad nebo korekturu obecného textu, pokud tím neporušují zadání nebo účel jazykové zkoušky.	Nechat AI automaticky oznámkovat esej, doporučit nepřijetí uchazeče nebo uzavřít podezření na podvod.
Vytvořit anonymizované příklady a poté je odborně zkontrolovat.	Aktivovat AI plugin v e-mailu, úložišti, LMS nebo prohlížeči bez schválení.
Použít chatbot pro obecné FAQ s jasným označením AI a eskalací na člověka.	Nechat chatbot odpovídat na individuální právně závazné, zdravotní, studijní nebo kázeňské otázky.
Použít AI jako pomůcku pro brainstorming a přiznat její použití podle zadání.	Odevzdat AI výstup jako vlastní práci nebo vytvořit falešné zdroje, data či důkazy.
Provést lidský přezkum AI doporučení a zdokumentovat závěr.	Používat rozpoznávání obličejů, detekci emocí, AI proctoring nebo kamerovou analytiku bez DPIA/FRIA a schválení.

Kontrolní otázky před použitím AI

- Je nástroj schválený pro tento konkrétní účel?
- Nevkládám osobní, citlivé, důvěrné nebo identifikovatelné údaje?
- Může výstup ovlivnit žáka, známku, přijetí, podporu nebo práva osoby?
- Dokážu výstup ověřit a převzít za něj odpovědnost?
- Byl žák nebo rodič přiměřeně informován?
- Mám možnost lidského přezkumu, námitky a nápravy?

Příloha č. 3: Karta AI systému / schvalovací formulář

Tento formulář se použije před zavedením nového AI systému, nové AI funkce nebo nového účelu použití již schváleného systému. U vysoce rizikového použití se doplní DPIA/FRIA a podrobnější dokumentace.

Název AI systému / funkce	
Dodavatel / provozovatel / verze	
Vlastník procesu ve škole	
Popis účelu použití	
Uživatelé systému	pedagogové / žáci / administrativa / veřejnost / jiné
Dotčené osoby	žáci / uchazeči / rodiče / zaměstnanci / veřejnost / jiné
Kategorie zpracovávaných údajů	
Obsahuje osobní údaje?	ano / ne / nejisté
Obsahuje zvláštní kategorie údajů nebo údaje dětí?	ano / ne / nejisté
AI Act kategorie	nižší riziko / transparentnost / vysoce rizikové / zakázané / mimo AI Act
Dopad na rozhodnutí o žákovi	žádný / podpůrný / významný / rozhodovací
Je nutná DPIA?	ano / ne / odůvodnění
Je nutná FRIA?	ano / ne / odůvodnění
Lidský dohled	kdo, kdy, jak zasahuje, jak se dokumentuje
Informační povinnost	kde a jak budou informováni žáci/rodiče/zaměstnanci
Smluvní režim	DPA / správce-správce / jiné; zákaz tréninku; subdodavatelé
Bezpečnostní opatření	SSO, MFA, role, logy, šifrování, retence, export, mazání
Výsledek schválení	schváleno / schváleno s podmínkami / pilot / zamítnuto
Datum revize	

Příloha č. 4: Checklist DPIA/FRIA pro AI ve školství

Otázka	Ano/Ne/Není relevantní	Poznámka / důkaz
Může AI ovlivnit přijetí, zařazení, hodnocení, studijní postup nebo kázeňské posouzení žáka?		
Zpracovává systém údaje nezletilých, zdravotní údaje, údaje o podpůrných opatřeních nebo jiné citlivé informace?		
Provádí systém profilování, predikci rizika, klasifikaci žáka nebo behaviorální analýzu?		
Používá systém obraz, zvuk, biometrické údaje, proctoring nebo kamerovou analytiku?		
Existuje méně invazivní alternativa se srovnatelným účelem?		
Jsou vstupní data relevantní, přesná, přiměřená a nediskriminační?		
Je zajištěn kvalifikovaný lidský dohled s možností změnit nebo odmítnout AI výstup?		
Jsou žáci/rodiče informováni srozumitelně a včas?		
Existuje proces námitky, vysvětlení, opravy a lidského přezkumu?		
Jsou definována logování, retence, přístupy, mazání a incident response?		
Je smluvně zakázán nepovolený trénink na datech školy?		
Byl posouzen dopad na žáky se speciálními vzdělávacími potřebami?		
Bylo provedeno pilotní testování přesnosti, bias a chybových scénářů?		

Příloha č. 5: Vzor informačního oznámení pro žáky a zákonné zástupce

[NÁZEV ŠKOLY] informuje žáky, uchazeče a zákonné zástupce, že v níže popsaném procesu může používat systém umělé inteligence. Cílem je transparentně vysvětlit, k čemu AI slouží, jaké údaje zpracovává, jak je zajištěn lidský dohled a jaká práva mají dotčené osoby.

Název AI systému	[doplnit]
Účel použití	[např. obecný chatbot / podpůrná analýza studijních dat / návrh zpětné vazby]
Jak AI ovlivňuje výsledek	[AI pouze pomáhá člověku / doporučuje / hodnotí podpůrně / neovlivňuje individuální rozhodnutí]
Kategorie údajů	[doplnit kategorie údajů]
Právní základ	[doplnit podle GDPR a školských předpisů]
Lidský dohled	[kdo výstup kontroluje a jak lze požádat o přezkum]
Možnost námitky nebo stížnosti	[kontakt a postup]
Doba uchování	[doplnit]
Dodavatel / příjemci	[doplnit]
Kontakt školy a DPO	[doplnit]

Doporučený krátký text pro web nebo LMS

„V některých procesech používáme AI jako podpůrný nástroj. AI nerozhoduje sama o vašem přijetí, hodnocení ani právech. Pokud AI významně pomáhá při posouzení, výsledek vždy kontroluje oprávněná osoba školy. Máte právo požádat o vysvětlení, opravu údajů, lidský přezkum nebo podat stížnost. Podrobnosti najdete v informačním oznámení školy.“

Příloha č. 6: Vzor záznamu o kontrole používání AI

Tento formulář slouží k dokumentaci přiměřené a transparentní kontroly souladu používání AI se směrnicí. Formulář je třeba přizpůsobit konkrétnímu případu, postavení osoby a zásadě minimalizace údajů.

Kontrolovaná osoba / útvar / kurz	
Datum a čas kontroly	
Místo / systém / zařízení	
Kontrolující osoby	
Důvod kontroly	
Právní a interní opora kontroly	
Předmět kontroly	

Kontrolní oblast	Zjištění	Opatření / termín
Schválení AI systému		
Použitý účet / licence		
Kategorie zpracovaných dat		
Dopad na žáka nebo hodnocení		
Nastavení sdílení a exportu		
Logování a auditní stopy		
Dodržení zásady minimalizace		
Lidský přezkum výstupů		
Informování dotčené osoby		
Incidenty / porušení		

Souhrnné vyhodnocení	
Navržená nápravná opatření	
Osoba odpovědná za nápravu	
Datum opětovného ověření	

Podpis kontrolující osoby: _____

Podpis kontrolované osoby / potvrzení seznámení: _____

Příloha č. 7: Potvrzení zaměstnance o seznámení se směrnicí

Níže podepsaná osoba potvrzuje, že byla seznámena se Směrnicí pro používání systémů umělé inteligence (AI) ve školství, rozumí jejím základním pravidlům a bere na vědomí, že při používání AI v pracovních souvislostech je povinna postupovat v souladu s touto směrnicí, souvisejícími interními předpisy a pokyny školy.

Jméno a příjmení	
Pracovní pozice / útvar	
Datum seznámení	
Forma seznámení	školení / e-learning / podpis / jiné
Podpis zaměstnance	
Podpis za školu	

Doporučení k evidenci

Potvrzení je vhodné evidovat společně s docházkou školení, onboardingovou dokumentací nebo v systému LMS. Pro žáky je vhodné pravidla AI zapracovat do školního řádu, pravidel předmětu, zadání prací a samostatného poučení v LMS.