CONSCIOUS YOUTH BEHAVIOURS
IN EMERGING REALITIES

R5. Odporúčanie k politike v oblasti bezpečnosti údajov a kybernetickej bezpečnosti, špeciálne prispôsobené pre školy, podľa noriem ISO 27001, 27002, 27701, 22301 a 31000

Vedomé správanie mládeže v rozvíjajúcich sa realitách

Vedúci partner : SIGMA BUSINESS NETWORK, Grécko

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Informácie o dokumente

Číslo grantovej zmluvy	**2023-1-EL01-KA220-SCH-000156982**
Skratka	**KYBERNETIKA**
Názov	**Vedomé správanie mládeže v vznikajúcich realitách**
Dátum začiatku:	16. 11. 2023
Výsledok:	Dokument s odporúčaniami pre politiku R5
Súvisiace aktivity:	A4.5 - Návrh a vývoj R5
Vedúca organizácia:	SIGMA Tournis Symvouleftiki EE, Grécko
Prispievajúci partneri:	• PRISM IMPRESA SOCIALE SRL , Taliansko • Krajské centrum pre vzdelávacie zdroje a pomoc Botoșani, Rumunsko • CPM-Centrum prevencie Mladeze, Slovensko • Casa Do Profesor, Portugalsko • Vitale Tecnologie Comunicazione - VITECO SRL, Taliansko • EUROCERT Eyropaiki Etaireia Emeghon Kai Pistopoihseon Anonymos Etaireia, Grécko
Úroveň šírenia	Verejné
Vyhlásenie o odmietnutí zodpovednosti	Podpora Európskej komisie pri vydaní tejto publikácie nepredstavuje schválenie jej obsahu, ktorý odráža iba názory autorov, a Komisia nenesie zodpovednosť za žiadne použitie informácií v nej obsiahnutých.

História dokumentu

Dátum	Odoslané používateľom	Recenzoval/a	Verzia (Poznámky)
26. 6. 2026	SIGMA	Theodora Ntinou	1,0

O spoločnosti CYBER	
Typ akcie	Erasmus+ KA220-SCH – Partnerstvá spolupráce v školskom vzdelávaní
Priorita	ŠKOLSKÉ VZDELÁVANIE: Rozvoj kľúčových kompetencií ▪ Riešenie digitálnej transformácie prostredníctvom rozvoja digitálnej pripravenosti, odolnosti a kapacity ▪ Inklúzia a rozmanitosť vo všetkých oblastiach vzdelávania, odbornej prípravy, mládeže a športu

Projekt sa zameriava na kľúčovú otázku: Ako kyberpriestor ovplyvňuje ľudské správanie, najmä medzi mladými ľuďmi? V dnešnej digitálnej dobe sa online správanie hlboko zakorenilo v psychologickom prostredí kyberpriestoru. Ponúka jedinečné príležitosti na formovanie ľudskej interakcie, ale zároveň vyvoláva obavy kvôli svojej bezhraničnej povahe. Hoci internet prináša nepopierateľné sociálne a ekonomické výhody, spochybňuje základné európske hodnoty, ako sú rovnosť, ľudské práva a demokracia. Na vybudovanie bezpečnejšieho internetu je nevyhnutné kolektívne úsilie. Zdieľanie osvedčených postupov a vzdelávanie mladých generácií, učiteľov a rodičov sú kľúčovými krokmi k podpore bezpečnejšieho online prostredia.

CYBER sa snaží rozvíjať kybernetickú odolnosť európskych škôl vytváraním prispôsobených postupov EÚ pre kvalitu školského systému a vybavením profesorov a študentov nástrojmi a vedomosťami na diskusiu o vedomom a nevedomom online správaní adolescentov, kyberpsychológii a nevýhodách nadmerného používania internetu s cieľom zlepšiť pochopenie tried o nebezpečnom vznikajúcom správaní, ktorému sa môže mladý používateľ vyskytnúť.

Projekt CYBER vypracuje metodiku na integráciu kľúčových tém kybernetických hrozieb a kyberpsychológie do tried a školského systému, čím podporí dialóg medzi študentmi o nebezpečnom objavujúcom sa správaní voči sebe a svojim rovesníkom. Projekt okrem toho stanovuje jasné postupy v oblasti kybernetickej ochrany a ochrany údajov, aby školy získali certifikáciu CYBER, a požiadavky na zavedenie, implementáciu, udržiavanie a zlepšovanie riadenia informačnej bezpečnosti v škole.

Výsledky projektu majú byť prínosom pre každého dospievajúceho v každej európskej krajine, najmä pre tých, ktorí sa narodili v digitálnej ére. Sociálny kontext v týchto záležitostiach (hackovanie profilov, falošné správy, falošné identity, online podvody, online vydieranie, pomstychtivá pornografia, hikikomori, kyberšikana atď.) má silnejšiu hodnotu, pričom vzdelávanie a informovanosť mladých ľudí o tomto probléme majú oveľa väčší vplyv ako národné pravidlá.

Obsah

Úvod

Tento dokument je Politika kybernetickej odolnosti škôl, ktorá bola vypracovaná ako súčasť projektu CYBER (Vedomé správanie mládeže v vznikajúcich realitách). Projekt je spolufinancovaný Európskou úniou v rámci programu Erasmus+ a združuje partnerské organizácie z Grécka, Talianska, Portugalska, Rumunska a Slovenska.

Školy sa dnes vo veľkej miere spoliehajú na digitálne technológie. Študenti používajú na učenie online platformy, učitelia komunikujú prostredníctvom digitálnych nástrojov a zamestnanci spravujú záznamy v prepojených systémoch. Je to pozitívny vývoj, ale zároveň to znamená, že školy čelia rizikám, ktorým predtým nečelili: kybernetickým útokom, únikom údajov, kyberšikane a vplyvu digitálneho života na duševné zdravie študentov.

Táto politika je navrhnutá tak, aby pomohla každej škole v piatich partnerských krajinách riešiť tieto výzvy praktickým spôsobom. Spája európske právo, vnútroštátne pravidlá každej krajiny, medzinárodne uznávané bezpečnostné normy a najlepší dostupný výskum, a to všetko v jednom dokumente, ktorý si môže prečítať a používať každá škola.

Toto nie je technická príručka. Je to sprievodca pre všetkých, ktorí pracujú v škole: riaditeľa, učiteľov, administratívnych pracovníkov a IT koordinátorov. Na jej používanie nepotrebujete právnické ani technické vzdelanie. Politika vysvetľuje, čo vyžaduje zákon, ako vyzerá osvedčený postup a čo musí vaša škola robiť.

Šablóny a nástroje uvedené v prílohách sú navrhnuté ako prispôsobiteľné východiskové body. Školy sa vyzývajú, aby ich upravili tak, aby vyhovovali ich národnému právnemu kontextu, interným postupom a špecifickým okolnostiam.

Pre koho sú tieto zásady určené

Tieto zásady sú určené pre všetkých, ktorí sa podieľajú na riadení školy: riaditeľa, zástupcu riaditeľa, učiteľov, koordinátorov IT, administratívnych pracovníkov školy a školské rady. Sú napísané tak, aby im rozumel každý bez ohľadu na jeho pôvod.

Ako je tento dokument usporiadaný

Časť	Obsah
Časť 1: Právny rámec	Čo musia školy robiť podľa európskeho práva, vysvetlené zrozumiteľne.
Časť 2: Pravidlá vašej krajiny	Konkrétne vnútroštátne pravidlá, ktoré platia v každej z piatich krajín.
Medzinárodné štandardy a školy	Ako päť medzinárodne uznávaných manažérskych štandardov formuje praktické odporúčania v tejto politike.
Časť 3: Čo by mala vaša škola urobiť	Praktické kroky usporiadané podľa témy, založené na medzinárodných normách a práve EÚ.

Časť	Obsah
Časť 4: Čo ukazujú dôkazy	Čo nám vedecký výskum hovorí o tom, čo v školách skutočne funguje.
Dodatky	Vzorové dokumenty a praktické implementačné nástroje, ktoré si školy môžu prispôsobiť a priamo používať.
Referencie	Vnútroštátne legislatívne nástroje a oficiálne zdroje použité pri príprave 2. časti.

Časť 1: Právny rámec

Školy vo všetkých piatich partnerských krajinách musia dodržiavať európske zákony, ktoré upravujú spôsob nakladania s údajmi a ochrany študentov online. Táto časť zrozumiteľne vysvetľuje, čo tieto zákony vyžadujú. Existuje šesť hlavných právnych nástrojov, o ktorých by mala každá škola vedieť. Spoločne zahŕňajú ochranu údajov, kybernetickú bezpečnosť, umelú inteligenciu, online platformy, digitálnu komunikáciu a bezpečnosť digitálnych produktov.

1.1 Všeobecné nariadenie o ochrane údajov (GDPR)

GDPR je základom ochrany údajov v Európe. Vzťahuje sa na každú organizáciu, ktorá spracováva osobné údaje, a to vrátane škôl. V škole osobné údaje zahŕňajú mená a identifikačné čísla študentov, záznamy o dochádzke, známky, zdravotné informácie, fotografie a akékoľvek ďalšie informácie, ktoré sa týkajú identifikovateľnej osoby.

GDPR uznáva deti ako obzvlášť zraniteľnú skupinu. Školy preto musia pri nakladaní s údajmi študentov uplatňovať vyšší štandard starostlivosti ako v prípade dospelých.

Čo GDPR vyžaduje od škôl:

- Školy by mali mať jasný právny základ pre každú činnosť spracovania údajov. Vo väčšine prípadov pôjde o zákonnú povinnosť vyžadovanú vnútroštátnym zákonom o vzdelávaní, verejnú úlohu potrebnú na prevádzku školy alebo v niektorých prípadoch o súhlas.
- Školy by mali zhromažďovať iba údaje, ktoré skutočne potrebujú. Nesmú zhromažďovať ďalšie informácie len preto, že by sa im jedného dňa mohli hodiť.
- Školy by mali vymenovať zodpovednú osobu pre ochranu údajov (DPO). V závislosti od krajiny sa to môže riadiť na úrovni orgánu alebo zoskupenia, a nie pre každú jednotlivú školu.
- Školy by mali pred zavedením akéhokoľvek nového digitálneho systému, ktorý zahŕňa rozsiahle spracovanie údajov o študentoch alebo monitorovanie správania, vykonať posúdenie vplyvu na ochranu údajov (DPIA). Šablóna je uvedená v dodatku V.
- Školy by mali nahlásiť porušenia ochrany osobných údajov národnému dozornému orgánu do 72 hodín od zistenia.
- Školy by mali informovať študentov a rodičov o tom, ako sa ich údaje používajú, a to jasným a zrozumiteľným jazykom.
- Študenti a rodičia majú právo na prístup k údajom, ktoré sa o nich uchovávajú, požadovať ich opravu a za určitých okolností aj vymazanie.

Vek digitálneho súhlasu

GDPR umožňuje každej krajine EÚ stanoviť vek, v ktorom môže mladá osoba súhlasiť s používaním digitálnych platforiem bez súhlasu rodičov. Tento vek sa v piatich partnerských krajinách pohybuje od 13 do 16 rokov. V prípade študentov, ktorí nedosiahli národný vek digitálneho súhlasu, musia školy pred zápisom na digitálne platformy získať písomný súhlas rodičov alebo zákonných zástupcov. Konkrétny vek pre každú krajinu je uvedený v časti 2.

1.2 Smernica NIS2

Smernica NIS2 stanovuje spoločný európsky rámec pre kybernetickú bezpečnosť. Vyžaduje od organizácií, aby mali zavedené primerané opatrenia v oblasti kybernetickej bezpečnosti, aby riadili riziká, ktoré predstavujú ich digitálni dodávatelia, a aby hlásili významné kybernetické incidenty vnútroštátnemu orgánu.

Školy nie sú v rámci NIS2 vždy priamo klasifikované ako základné alebo dôležité subjekty. Školy však vo veľkej miere závisia od digitálnych systémov a kybernetické incidenty ovplyvňujúce tieto systémy môžu narušiť vzdelávanie a ohroziť údaje študentov. Rámec NIS2 stanovuje štandard, o ktorý by sa mali usilovať všetky školy bez ohľadu na to, či sú formálne klasifikované, či už sú formálne klasifikované.

Čo NIS2 znamená pre školy:

- Školy by mali zaviesť opatrenia kybernetickej bezpečnosti, ktoré zodpovedajú rizikám, ktorým čelia. Minimálne to znamená silné heslá, pravidelné zálohy a chránené siete.
- Školy by mali skontrolovať postupy kybernetickej bezpečnosti svojich digitálnych dodávateľov. Platforma používaná pre záznamy študentov musí byť rovnako bezpečná ako samotná škola.
- Školy by mali mať postup na odhaľovanie a reakciu na kybernetické bezpečnostné incidenty. Zamestnanci musia vedieť, na koho sa majú obrátiť a aké kroky majú dodržiavať.
- Školy by mali poskytovať pravidelné školenia o kybernetickej bezpečnosti pre všetkých zamestnancov.
- Významné incidenty by sa mali hlásiť národnému orgánu kybernetickej bezpečnosti. Lehoty a orgány sa v jednotlivých krajinách líšia. Pozri 2. časť.

1.3 Zákon EÚ o umelej inteligencii

Zákon o umelej inteligencii (AI Act) je prvý komplexný európsky zákon upravujúci používanie umelej inteligencie. Nadobudol účinnosť v auguste 2024 a postupne sa uplatňuje až do úplnej implementácie v auguste 2026. Školy čoraz viac využívajú nástroje podporované umelou inteligenciou: adaptívne vzdelávacie platformy, automatizované systémy hodnotenia, chatboty a analytiku vzdelávania. Zákon o umelej inteligencii vytvára jasné pravidlá pre to, ako sa tieto nástroje môžu a nemôžu používať.

Čo zákon o umelej inteligencii vyžaduje od škôl:

- Niektoré spôsoby použitia umelej inteligencie v školách sú úplne zakázané. Patria sem systémy rozpoznávania emócií používané na monitorovanie študentov, biometrická kategorizácia študentov a rozpoznávanie tváre v reálnom čase vo vzdelávacích zariadeniach. Pre školy neexistujú žiadne výnimky.

- Systémy umelej inteligencie používané na hodnotenie, prijímanie alebo monitorovanie študentov sú klasifikované ako vysoko rizikové a musia spĺňať prísne požiadavky na transparentnosť, ľudský dohľad a dokumentáciu.
- Študenti a rodičia by mali byť informovaní o tom, kedy sa nástroje umelej inteligencie používajú spôsobmi, ktoré ovplyvňujú rozhodnutia v oblasti vzdelávania.
- Učiteľ by mal vždy skontrolovať a prevziať zodpovednosť za akékoľvek odporúčania vygenerované umelou inteligenciou, ktoré ovplyvňujú študenta. Umelá inteligencia nemôže robiť konečné rozhodnutia o študentoch.
- Školy by mali viesť písomný zoznam všetkých používaných nástrojov umelej inteligencie vrátane toho, čo každý nástroj robí a aké údaje spracováva.

1.4 Zákon o digitálnych službách (DSA)

Zákon o digitálnych službách (DSA) reguluje online platformy a digitálne služby. Vyžaduje si, aby boli platformy transparentnejšie, aby poskytovali dostupné spôsoby nahlasovania škodlivého obsahu a aby posilnili ochranu mladých ľudí. Školy zohrávajú dôležitú úlohu pri pomáhaní študentom pochopiť, ako online platformy fungujú a ako sa chrániť.

Čo DSA znamená pre školy:

- Školy by mali študentov učiť, ako rozpoznať a nahlásiť škodlivý obsah na platformách, ktoré používajú.
- Školy by mali študentom pomôcť pochopiť, ako fungujú algoritmy odporúčaní a ako formujú to, čo mladí ľudia vidia online.
- Učitelia by si mali byť vedomí povinností, ktoré DSA ukladá hlavným platformám, a mali by byť schopní o nich diskutovať so študentmi v rámci vzdelávania v oblasti digitálnej gramotnosti.

1.5 Smernica o elektronickom súkromí

Smernica o súkromí a elektronických komunikáciách chráni dôvernosť elektronickej komunikácie. Vzťahuje sa na e-mailové systémy, platformy na odosielanie správ, nástroje na videokonferencie a akékoľvek iné digitálne komunikačné služby používané v školách.

Čo znamená smernica o súkromí a elektronických komunikáciách pre školy:

- Digitálna komunikácia medzi študentmi, rodičmi, učiteľmi a administratívnymi pracovníkmi by mala byť bezpečná a dôverná.
- Nástroje na videokonferencie používané na dištančné vzdelávanie by mali byť nakonfigurované tak, aby sa zabránilo neoprávnenému prístupu. Virtuálne učebne by mali vyžadovať prihlásenie pred pripojením sa kohokoľvek.
- Lekcie a stretnutia by sa nemali nahrávať bez výslovného súhlasu všetkých účastníkov.
- Školské webové stránky a platformy, ktoré používajú súbory cookie, by mali zobrazovať oznámenie o súboroch cookie v súlade s predpismi.

1.6 Zákon o kybernetickej bezpečnosti

Zákon o kybernetickej bezpečnosti posilňuje úlohu ENISA, Agentúry EÚ pre kybernetickú bezpečnosť, a zavádza európsky rámec pre certifikáciu digitálnych produktov a služieb ako bezpečných. Podporuje zavádzanie dôveryhodných technológií v celej EÚ, a to aj v školách.

Čo znamená zákon o kybernetickej bezpečnosti pre školy:

- Pri výbere digitálnych nástrojov, platforiem alebo zariadení by školy mali zohľadniť kybernetickú bezpečnosť a podľa možnosti uprednostňovať certifikované alebo schválené produkty.
- Pripojené zariadenia v triede, ako sú inteligentné tabule, tablety a kamery, by mali byť bezpečne nakonfigurované a udržiavané aktualizované.
- Školy si môžu na plánovanie svojho prístupu k kybernetickej bezpečnosti pozrieť usmernenia a nástroje agentúry ENISA.

1.7 Ako tieto zákony fungujú spoločne

Týchto šesť právnych nástrojov nepredstavuje samostatné povinnosti, ktoré by sa mali riešiť jednotlivo. Tvoria integrovaný rámec. Škola, ktorá chráni údaje študentov podľa GDPR, riadi kybernetickú bezpečnosť podľa NIS2, zodpovedne používa umelú inteligenciu podľa zákona o umelej inteligencii, vyučuje digitálnu gramotnosť v súlade so zákonom DSA, zabezpečuje svoju komunikáciu podľa smernice o elektronickom súkromí a vyberá dôveryhodné technológie v súlade so zákonom o kybernetickej bezpečnosti, bude mať splnené všetky svoje zákonné povinnosti.

Právo	Kľúčová povinnosť škôl
GDPR	Chráňte osobné údaje, vymenujte zodpovednú osobu, v prípade potreby získajte súhlas a nahláste porušenia do 72 hodín.
Smernica NIS2	Majte zavedené opatrenia v oblasti kybernetickej bezpečnosti, kontrolujte svojich dodávateľov, hláste incidenty, školte svojich zamestnancov.
Zákon EÚ o umelej inteligencii	Nepoužívajte zakázanú umelú inteligenciu, nechajte rozhodovanie na ľudí, informujte študentov a rodičov.
Zákon o digitálnych službách	Naučte študentov nahlasovať škodlivý obsah a pochopiť, ako fungujú algoritmy.
Smernica o súkromí a elektronických komunikáciách	Zabezpečte digitálnu komunikáciu, chráňte virtuálne učebne, dodržiavajte pravidlá používania súborov cookie.
Zákon o kybernetickej bezpečnosti	Pri kúpe technológií zvážte bezpečnosť, zabezpečte pripojené zariadenia a využite usmernenia agentúry ENISA.

Časť 2: Čo platí vo vašej krajine

Európske právo stanovuje spoločný rámec, ale každá krajina má aj vlastné vnútroštátne zákony a usmernenia, ktoré musia školy dodržiavať. Táto časť sumarizuje najdôležitejšie vnútroštátne pravidlá pre každú z piatich partnerských krajín. Nájdite si svoju krajinu a overte si, čo sa na vás vzťahuje.

2.1 Grécko

Grécko prevádzkuje vysoko centralizovaný model digitálnej správy škôl. Kybernetickú bezpečnosť, ochranu údajov a digitálnu infraštruktúru riadi predovšetkým na národnej úrovni ministerstvo školstva a ministerstvo digitálnej správy. Jednotlivé školy fungujú najmä ako používatelia centrálne spravovaných systémov vrátane študentského informačného systému MySchool, vzdelávacej platformy e-Class a Panhelénskej školskej siete (PSN).

Oblasť	Čo to znamená pre školy
Transpozícia NIS2 Zákon 5160/2024 MD 1689/2025 MD 1899/2025	• Školy musia zaviesť opatrenia na riadenie rizík a zabezpečiť, aby digitálne platformy tretích strán (napr. Webex) spĺňali štandardy kybernetickej bezpečnosti. • Povinné hlásenie incidentov: školy musia informovať EAKE o významných kybernetických bezpečnostných incidentoch. • Vyžadujú sa formálne bezpečnostné zásady, ktoré zahŕňajú kontrolu prístupu k údajom študentov, postupy zálohovania, šifrovanie komunikácie a zabezpečenie dodávateľského reťazca pre softvér a hardvér používaný v školách. • Vyžaduje sa školenie zamestnancov a kybernetická hygiena: školský personál je častým cieľom phishingových útokov a útokov sociálneho inžinierstva. • Školy musia viesť dokumentáciu vrátane bezpečnostných politík, záznamov o školeniach, sieťových diagramov a výsledkov pravidelných bezpečnostných auditov. • Nariadenie MD 1899/2025 vyžaduje určenie zodpovednej osoby za kybernetickú bezpečnosť a formálne postupy reakcie na incidenty a eskalácie.
Ochrana údajov Zákon 4624/2019	• Upravuje spracovanie osobných údajov orgánmi verejného sektora vrátane škôl v súlade so zásadami GDPR. • Stanovuje úlohu a dozorné právomoci Gréckeho úradu pre ochranu údajov (HDPA). • Zodpovednosti DPO sú riadené na úrovni orgánov, a nie pre každú jednotlivú školu. • Školy musia do 72 hodín informovať HDPA (Hélsky úrad pre ochranu údajov) o akomkoľvek porušení ochrany osobných údajov, ktoré by mohlo predstavovať riziko pre jednotlivcov. • Školy musia zaviesť vhodné bezpečnostné opatrenia pre údaje študentov, rodičov a zamestnancov.
Vek digitálneho súhlasu	• 15 rokov. • Školy musia pred zápisom žiakov mladších ako 15 rokov na akúkoľvek digitálnu platformu, ktorá spracováva ich osobné údaje, získať písomný súhlas rodičov alebo zákonných zástupcov.
Kyberšikana Zákon 5029/2023	• Poskytuje štruktúrovaný právny rámec pre prevenciu a riadenie kyberšikany v školách. • Zavádza národnú platformu pre hlásenie šikany stop-bullying.gov.gr na formálne nahlasovanie a sledovanie incidentov.

Oblasť	Čo to znamená pre školy
	• Školy sa musia aktívne podieľať na identifikácii, hlásení a riešení prípadov kyberšikany. • Školy musia mať písomný postup pre reakciu na incidenty kyberšikany.
Mobilné telefóny	• Žiakom je zakázané vlastniť alebo používať mobilné telefóny v priestoroch školy. • Politika nulovej tolerancie platná od roku 2024. • Porušenia majú okamžité disciplinárne dôsledky vrátane pozastavenia činnosti.
UI vo vzdelávaní	• Pre používanie umelej inteligencie v školách neboli vydané žiadne špecifické národné usmernenia. • Zákon EÚ o umelej inteligencii sa uplatňuje priamo. • Školy by mali byť opatrné pri používaní nástrojov umelej inteligencie, ktoré spracovávajú údaje študentov.
Digitálna infraštruktúra	• MySchool: národný študentský informačný systém, centrálne spravovaný. • e-Class: národná platforma pre riadenie vzdelávania. • Panhelénska školská sieť (PSN): bezpečná národná infraštruktúra prepojenia pre všetky verejné školy.
Kľúčové kontakty	• Kybernetická bezpečnosť: EAKE (cyber.gov.gr) • Ochrana údajov: HDPA (dpa.gr) • Kyberšikana: stop-bullying.gov.gr

2.2 Taliansko

Taliansko prevádzkuje prevažne centralizovaný model, hoci školy si zachovávajú určitý stupeň organizačnej autonómie. Národná agentúra pre kybernetickú bezpečnosť (ACN) zohráva ústrednú úlohu v koordinácii a riadení incidentov. Školy sú vo veľkej miere závislé od ministerského usmernenia a centrálne riadených platforiem vrátane národnej platformy Unica. Agentúra Garante vydala usmernenia a často kladené otázky špecifické pre školy, ktoré by si školy mali preštudovať popri GDPR.

Oblasť	Čo to znamená pre školy
Transpozícia NIS2 Legislatívny dekrét 138/2024 Zákon 109/2021	• Legislatívny dekrét 138/2024 formuje očakávania týkajúce sa hodnotenia rizík, bezpečnosti dodávateľov a hlásenia incidentov, a to aj pre školy, ktoré nie sú priamo klasifikované ako subjekty NIS. • Školy musia riadiť služby IKT tretích strán a udržiavať štruktúrované kanály nahlasovania, keď incidenty ovplyvňujú vzdelávacie aktivity alebo údaje študentov. • Zákonom č. 109/2021 sa zriaďuje Národná agentúra pre kybernetickú bezpečnosť (ACN), ktorá zohráva ústrednú

Oblasť	Čo to znamená pre školy
	koordinačnú úlohu v oblasti riadenia kybernetickej bezpečnosti vo verejných inštitúciách vrátane škôl.
Ochrana údajov Legislatívny dekrét 196/2003 (v znení vyhlášky č. 101/2018)	• Upravuje spracovanie údajov študentov, rodičov, učiteľov a zamestnancov v rámci školských aktivít. • Dozorným orgánom je Garante per la protezione dei dati personali. • Určenie DPO je povinné pre verejné školy, ale môže byť organizované na úrovni školy alebo prostredníctvom spoločných dohôd medzi viacerými školami. • Na spracovanie údajov detí, ak sú digitálne služby ponúkané priamo študentom, ktorí nedosiahli vek digitálneho súhlasu, sa vyžaduje súhlas rodičov. • Školy musia informovať študentov a rodičov o ich právach na ochranu údajov a riešiť úniky údajov v súlade s požiadavkami GDPR.
Vek digitálneho súhlasu	• 14 rokov. • Súhlas rodičov sa vyžaduje pre študentov mladších ako 14 rokov na zápis do systémov riadenia vzdelávania, zverejňovanie fotografií a akékoľvek spracovanie údajov, ktoré sa týka maloletých osôb vo vzdelávacom prostredí.
Kyberšikana Zákon 71/2017	• Poskytuje právny rámec pre boj proti kyberšikane v školách. • Školy musia mať písomné postupy na riešenie incidentov a podporu obetí. • Školy môžu požiadať o odstránenie škodlivého obsahu z online platforiem.
Mobilné telefóny Poznámka MIM 5274/2024 Obežník MIM 3392/2025	• Používanie smartfónov je obmedzené počas všetkých školských aktivít vo všetkých vzdelávacích cykloch. • Cieľom obmedzení je chrániť vzdelávacie prostredie a podporovať veku primerané používanie digitálnych nástrojov. • Obmedzené výnimky platia pre špecifické vzdelávacie aktivity alebo potreby prístupnosti.
UI vo vzdelávaní Ministerský dekrét 166/2025	• Národné smernice vyžadujú transparentnosť v oblasti používania umelej inteligencie v školách. • Ľudský dohľad nad vzdelávacími rozhodnutiami podporovanými umelou inteligenciou je povinný. • Nástroje umelej inteligencie, ktoré spracovávajú údaje študentov, musia spĺňať požiadavky GDPR.
Digitálne platformy	• Unica: národná platforma pre administratívne a vzdelávacie funkcie. • Microsoft 365 pre vzdelávanie: inštitucionálne spravovaný balík pre výučbu a komunikáciu.

Oblasť	Čo to znamená pre školy
	• Rámec digitálne integrovaného vyučovania (DDI) (MD 89/2020) vyžaduje, aby školy regulovali používanie digitálnych platforiem, prístup študentov a zodpovednosti učiteľov v online vzdelávacích prostrediach.
Kľúčové kontakty	• Kybernetická bezpečnosť: ACN (acn.gov.it) • Ochrana údajov: Garante (garanteprivacy.it)

2.3 Portugalsko

Portugalsko má jeden z najštruktúrovanejších národných rámcov pre digitálne riadenie škôl spomedzi piatich krajín. Školy využívajú povinný program PADDE (Akčný plán digitálneho rozvoja škôl), podporný program SeguraNet a CERT.PT pre reakciu na incidenty. Smernica NIS2 bola transponovaná prostredníctvom dekrétu-zákona 125/2025, ktorý nadobudol účinnosť 3. apríla 2026.

Oblasť	Čo to znamená pre školy
Transpozícia NIS2 Zákonný dekrét 125/2025 (účinné od 3. apríla 2026) Zákon 46/2018	• Školy, ktoré sa kvalifikujú ako relevantné verejné subjekty (skupina A alebo B), musia zaviesť opatrenia na riadenie kybernetických bezpečnostných rizík. • Povinné určenie zodpovednej osoby pre kybernetickú bezpečnosť. • Závažné incidenty musia byť nahlásené CNCS do 24 hodín. • Školy musia identifikovať kritické digitálne aktíva, zaviesť postupy reakcie na incidenty a zabezpečiť kontinuitu prevádzky. • Zákon 46/2018 zostáva základným rámcom, ktorým sa CNCS zriaďuje ako národný orgán kybernetickej bezpečnosti.
Ochrana údajov Zákon 58/2019	• Zodpovedná osoba za ochranu údajov je povinná na úrovni každého školského zoskupenia (agrupamento de escolas), nie jednotlivých škôl. • DPO musí byť zaregistrovaný v CNPD (Comissão Nacional de Proteção de Dados) a je zodpovedný za monitorovanie súladu s GDPR, poradenstvo personálu, vedenie školení a styk s CNPD. • Školy musia oznámiť CNPD do 72 hodín o porušení ochrany osobných údajov, ktoré pravdepodobne predstavuje riziko pre jednotlivcov. • Školy musia viesť register činností spracovania a zaviesť vhodné bezpečnostné opatrenia.
Vek digitálneho súhlasu	• 13 rokov. Toto je najnižšia hranica spomedzi piatich krajín. • Pred zápisom študentov mladších ako 13 rokov na akúkoľvek digitálnu platformu alebo online nástroj, ktorý spracúva osobné údaje, sa vyžaduje overiteľný súhlas rodičov alebo zákonných zástupcov.

Oblasť	Čo to znamená pre školy
	• Toto sa vzťahuje na systémy riadenia vzdelávania, zverejňovanie fotografií a akékoľvek spracovanie údajov, ktoré sa týka maloletých.
Kyberšikana Program SeguraNet	• SeguraNet (spravovaný spoločnosťou DGE v spolupráci s CNCS) poskytuje konkrétne usmernenia týkajúce sa prevencie a reakcie na kyberšikanu. • Školy musia integrovať prevenciu kyberšikany do svojich PADDE a interných predpisov. • Vzorové postupy reakcie na incidenty a dokumenty o zásadách prijateľného používania sú k dispozícii prostredníctvom siete SeguraNet.
Mobilné telefóny Zákonný dekrét 95/2025 (platné od septembra 2025)	• Smartfóny sú zo zákona zakázané pre všetkých žiakov 1. až 6. ročníka vo všetkých verejných aj súkromných školách. • Pre 3. cyklus a stredné školy ministerstvo vydalo odporúčania podporujúce obmedzenia, pričom školy si ponechali autonómiu pri formalizácii pravidiel vo svojich interných predpisoch. • Akékoľvek nahrávanie študentov vyžaduje podľa GDPR výslovný súhlas.
Povinný školský digitálny plán Rámec PADDE	• Každý školský klaster musí vypracovať a udržiavať PADDE (Akčný plán digitálneho rozvoja školy). • PADDE musí výslovne zahŕňať opatrenia v oblasti kybernetickej bezpečnosti a pokrýva tri rozmery: organizačný (vedenie a riadenie), pedagogický (digitálne občianstvo a vzdelávanie v oblasti bezpečného internetu) a technologický (infraštruktúra a bezpečnosť). • Školy musia prijať politiku prijateľného používania a zaviesť postupy reakcie na incidenty s odkazom na CERT.PT.
UI vo vzdelávaní	• Zatiaľ neboli vydané žiadne konkrétne národné usmernenia. • Zákon EÚ o umelej inteligencii sa uplatňuje priamo. • Generálny riaditeľ pre environmentálnu politiku (DGE) uznal potrebu národného rámca a očakáva sa, že vydá odporúčania. • Školy by mali byť opatrné pri používaní nástrojov umelej inteligencie, ktoré spracovávajú údaje študentov.
Digitálna infraštruktúra	• RCTS (spravovaná FCCN): národná vysokorýchlostná zabezpečená sieť pre všetky klastre verejných škôl. • Microsoft 365 pre vzdelávanie: národne spravovaný balík pre výučbu a komunikáciu. • CERT.PT (prevádzkovaný spoločnosťou CNCS): národný kontakt CSIRT a reakcie na incidenty pre sektor vzdelávania.
Kľúčové kontakty	• Kybernetická bezpečnosť: CNCS (cncs.gov.pt) • Reakcia na incident: CERT.PT • Ochrana údajov: CNPD (cnpd.pt)

Oblasť	Čo to znamená pre školy
	• Digitálna bezpečnosť: SeguraNet (seguranet.pt)

2.4 Rumunsko

Národný rámec koordinuje ministerstvo školstva v spolupráci s Národným riaditeľstvom pre kybernetickú bezpečnosť (DNSC) v rámci širšieho národného a európskeho rámca politiky kybernetickej bezpečnosti. V mnohých školách preberá zodpovednosť za kybernetickú bezpečnosť riaditeľ školy, koordinátor IKT alebo určený učiteľ, keďže špecializovaní zamestnanci v oblasti kybernetickej bezpečnosti sú zriedkaví. Rumunsko čelí niektorým z najväčších implementačných nedostatkov spomedzi piatich partnerských krajín, ale narastá dynamika ich riešenia.

Oblasť	Čo to znamená pre školy
Transpozícia NIS2 OUG 155/2024 (schválené zákonom 124/2025) Zákon 58/2023	• Nariadenie OUG 155/2024 sa priamo vzťahuje na vysokoškolské vzdelávanie. V prípade preduniverzitných škôl nie je uplatniteľnosť úplne jasná, ale od škôl, ktoré interagujú s vládnymi sieťami (napr. SIIIR), sa očakáva, že budú dodržiavať protokoly NIS2. • Od škôl sa očakáva, že nahlásia závažné incidenty DNSC do 24 hodín prostredníctvom platformy PNRISC. • Medzi požadované opatrenia patrí: segmentácia siete (samostatné Wi-Fi pre administratívu a študentov), viacfaktorové overovanie pre prístup k oficiálnym platformám, zásady analýzy rizík a povinné školenie v oblasti kybernetickej hygieny pre všetkých zamestnancov. • Bezpečnosť dodávateľského reťazca: súkromní dodávatelia platforiem elektronického vzdelávania alebo účtovného softvéru používaného školami musia byť v súlade s NIS2. • Zákon 58/2023 stanovuje, že zodpovednosť za kybernetickú bezpečnosť nesie subjekt, ktorý vlastní alebo spravuje sieť, čím sa za ňu priamo zodpovedá vedenie školy.
Ochrana údajov Zákon 190/2018	• Školy sú klasifikované ako nezávislí prevádzkovatelia údajov a musia zabezpečiť úplný súlad s GDPR. • Spoločná dohoda o zodpovednej osobe je povolená na úrovni okresného inšpektorátu alebo ústredného orgánu. • Školy musia zaviesť povinné postupy súhlasu rodičov s online vzdelávacími platformami a s používaním obrázkov študentov. • Video monitorovanie je povolené len na ochranu osôb a majetku s povinným informovaním študentov, učiteľov a návštevníkov. Záznamy sa nesmú uchovávať dlhšie ako 30 dní, s výnimkou vyšetrovaných incidentov. • Výsledky skúšok musia byť zverejnené s použitím anonymizácie alebo pseudonymizácie v súlade s pokynmi ANSPDCP.

Oblasť	Čo to znamená pre školy
Vek digitálneho súhlasu	• 16 rokov. Toto je najvyššia hranica spomedzi piatich krajín. • Pred zápisom študentov mladších ako 16 rokov na akúkoľvek digitálnu platformu je potrebný súhlas rodiča alebo zákonného zástupcu. • V praxi sa to týka prakticky všetkých digitálnych vzdelávacích nástrojov používaných v rumunských školách.
Kyberšikana ROFUIP 2025/2026 Študentský štatút (Nariadenie 5707/2024)	• ROFUIP definuje a trestá kyberšikanu ako zakázané správanie v školskom prostredí. • Neoprávnené video alebo audio nahrávanie vyučovacích aktivít je zakázané. • Zamestnanci by mali používať iba oficiálne schválené digitálne nástroje a s údajmi študentov by mali zaobchádzať prísne dôverne. • Študentský štatút výslovne zakazuje akúkoľvek formu agresie vo virtuálnom prostredí. • Neexistuje žiadna špecializovaná národná platforma na podávanie hlásení. Incidenty rieši škola a v prípade osobných údajov sa postupujú ANSPDCP.
Mobilné telefóny Zákon 198/2023 ROFUIP	• Používanie mobilných telefónov počas vyučovania je pre žiakov predškolských, základných a nižších stredných škôl zakázané, s výnimkou prípadov, keď to učiteľ povolí na vzdelávacie účely. • Telefóny musia byť počas vyučovania vypnuté alebo v tichom režime a uložené na určenom mieste podľa ROFUIP. • Pravidlá používania telefónu počas prestávok sú stanovené vnútornými predpismi každej školy.
UI vo vzdelávaní	• Neboli vydané žiadne konkrétne národné usmernenia. Priamo sa uplatňuje zákon EÚ o umelej inteligencii. • Ministerstvo školstva nevydalo usmernenia k generatívnym nástrojom umelej inteligencie, ako je ChatGPT, čím vzniká značná medzera. • Školy by mali pri používaní akéhokoľvek nástroja umelej inteligencie so študentmi uplatňovať požiadavky zákona o umelej inteligencii týkajúce sa transparentnosti, ľudského dohľadu a ochrany údajov.
Digitálna infraštruktúra	• Neexistuje jednotná národná školská sieť. Školy sa spoliehajú na komerčných poskytovateľov internetu, čo vedie k nejednotným štandardom kybernetickej bezpečnosti. • SIIIR (centrálne spravovaná ministerstvom) je hlavná národná databáza údajov o študentoch. • Školy využívajú komerčné platformy (Google Workspace, Microsoft 365) na základe individuálnych zmlúv.
Kľúčové kontakty	• Kybernetická bezpečnosť: DNSC (dnsc.ro) • Ochrana údajov: ANSPDCP (dataprotection.ro)

2.5 Slovensko

Slovensko preukázalo silný legislatívny impulz v oblasti digitálneho riadenia škôl. Zákon o kybernetickej bezpečnosti č. 366/2024, obmedzenia mobilných telefónov platné od januára 2025, špecializované usmernenia týkajúce sa kyberšikany (Usmernenie č. 1/2025) a národný plán umelej inteligencie vo vzdelávaní na roky 2025 až 2027 odrážajú komplexný a štruktúrovaný prístup. Riaditeľ školy nesie priamu právnu zodpovednosť za kybernetickú bezpečnosť podľa slovenského práva. Infraštruktúrny program DigiEDU/DigiNET poskytuje bezpečné a centralizované internetové pripojenie všetkým slovenským školám.

Oblasť	Čo to znamená pre školy
Transpozícia NIS2 Zákon 366/2024 Zákon č. 69/2018	• Zákon č. 366/2024 priamo spája povinnosti v oblasti kybernetickej bezpečnosti so zákonnou zodpovednosťou riaditeľa školy podľa zákona č. 596/2003 o školách. Riaditeľ je osobne a právne zodpovedný za ochranu školských informačných systémov a osobných údajov. • Školy musia zaviesť základné bezpečnostné opatrenia: silné heslá, antivírusový softvér, pravidelné aktualizácie, zálohovanie údajov a kontrolu prístupu. • Školy musia byť schopné reagovať na phishingové útoky, ransomvér, úniky údajov a narušenia systému. • V prípade závažných kybernetických bezpečnostných incidentov sa musia dodržiavať povinné postupy hlásenia. • Zákon č. 69/2018 poskytuje základný rámec pre ochranu informačných systémov a sietí, zabezpečuje bezpečnosť údajov študentov a bezpečné používanie digitálnych technológií v školách.
Ochrana údajov Zákon č. 18/2018	• Zodpovedná osoba za ochranu údajov je povinná pre verejné školy, ale nemusí byť jedna na školu: spoločná ZO pre viacero škôl je povolená. • Školy musia uplatňovať minimalizáciu údajov: zhromažďovať a používať iba osobné údaje študentov, ktoré sú nevyhnutne potrebné na vzdelávanie a administratívu. • Prístup k údajom musí byť podľa potreby obmedzený na oprávnené osoby (učitelia, vedenie, administratíva). • Elektronické systémy, e-maily, papierové dokumenty a pamäťové zariadenia musia byť chránené pred stratou alebo neoprávneným prístupom. • Fotografie, zoznamy študentov, výsledky ani citlivé informácie nesmú byť zverejnené bez právneho základu alebo výslovného súhlasu. • Akékoľvek porušenie ochrany údajov musí byť nahlásené príslušnému orgánu do 72 hodín, ak predstavuje riziko pre jednotlivcov.
Vek digitálneho súhlasu	• 16 rokov.

Oblasť	Čo to znamená pre školy
	• Pred zápisom študentov mladších ako 16 rokov na digitálne platformy je potrebný súhlas rodiča alebo zákonného zástupcu.
Kyberšikana Usmernenie 1/2025	• Usmernenie 1/2025 stanovuje konkrétne pravidlá týkajúce sa prevencie a riešenia kyberšikany v školách a vzdelávacích zariadeniach. • Definuje základné znaky, formy a prejavy kyberšikany. • Stanovuje preventívne postupy a metódy riešenia incidentov. • Zahŕňa postupy na podporu obetí. • Školy musia implementovať postupy stanovené v tomto usmernení.
Mobilné telefóny Zákon č. 245/2008 (zmenené a doplnené od januára 2025)	• Žiaci 1. až 3. ročníka nesmú počas vyučovania vôbec používať mobilné telefóny ani podobné zariadenia. • Žiaci 4. až 9. ročníka ich môžu používať len na vzdelávacie účely, ak im to učiteľ výslovne povolí. • Výnimka platí pre študentov so zdravotným postihnutím, ktorí používajú zariadenie v súvislosti so svojím zdravotným stavom. • V prípade porušenia môže škola zariadenie dočasne zabaviť. • Podrobné podmienky upravujú vnútorné predpisy školy.
UI vo vzdelávaní Plán umelej inteligencie na roky 2025 – 2027	• Plán ministerstva školstva pre zodpovedné využívanie umelej inteligencie vo vzdelávaní na roky 2025 – 2027 poskytuje praktické národné usmernenia pre školy. • Školy by mali tento plán používať spolu so zákonom EÚ o umelej inteligencii na posudzovanie a riadenie akýchkoľvek nástrojov umelej inteligencie, ktoré zavádzajú. • Dôraz sa kladie na bezpečnosť, etické používanie a transparentnosť.
Digitálna infraštruktúra	• DigiEDU/DigiNET: bezpečný, centrálne spravovaný program internetového pripojenia pre všetky slovenské školy. • Kybernetickú bezpečnosť dohliada Národný bezpečnostný úrad (NBU), ktorý prevádzkuje SK-CERT pre reakciu na incidenty. • NBU poskytuje poradenstvo a podporu verejným inštitúciám vrátane škôl.
Kľúčové kontakty	• Kybernetická bezpečnosť: NBU/SK-CERT (nbu.gov.sk) • Ochrana údajov: ÚOOU (dataprotection.gov.sk)

Medzinárodné štandardy a školy

Praktické odporúčania v 3. časti tejto politiky sú založené na súbore medzinárodne uznávaných manažérskych štandardov. Táto krátka časť vysvetľuje, čo tieto štandardy sú a prečo sú pre školy dôležité. Na to, aby ste sa riadili pokynmi v 3. časti, nemusíte poznať samotné štandardy. Štandardy poskytujú overený a široko akceptovaný základ, ktorý dáva tejto politike jej štruktúru a dôveryhodnosť.

Relevantných je tu päť štandardov. Každý z nich sa zaoberá iným aspektom toho, ako môžu školy chrániť svojich študentov, ich údaje a ich systémy.

Norma ISO/IEC 27001 je medzinárodná norma pre riadenie informačnej bezpečnosti. Poskytuje rámec na identifikáciu informácií, ktoré škola uchováva, pochopenie rizík pre tieto informácie a zavedenie správnych opatrení na ich ochranu. V kontexte školy to znamená záznamy o študentoch, údaje o zamestnancoch, digitálne platformy a všetky systémy, ktoré podporujú výučbu a administratívu. Norma ISO 27001 nepredpisuje konkrétne technické riešenia. Namiesto toho stanovuje spôsob systematického uvažovania o bezpečnosti, pričom sa zabezpečí, aby sa nič dôležité neprehliadlo. Praktické kroky v častiach 3.1 až 3.7 vychádzajú z tohto rámca.

Norma ISO/IEC 27002 je súčasťou normy ISO 27001 a poskytuje podrobné kontroly, ktoré zavádzajú informačnú bezpečnosť do praxe. Zatiaľ čo norma ISO 27001 opisuje rámec riadenia, norma ISO 27002 popisuje konkrétne opatrenia: ako kontrolovať prístup k systémom, ako spravovať heslá, ako riešiť incidenty, ako bezpečne konfigurovať zariadenia. Časti 3.2 a 3.3 čerpajú z tejto normy najpriamejšie.

Norma ISO/IEC 27701 rozširuje rámec informačnej bezpečnosti tak, aby sa vzťahovala najmä na ochranu osobných údajov. Priamo nadväzuje na GDPR a pomáha školám preukázať, že zodpovedne spravujú údaje študentov a zamestnancov. Časť 3.1 je postavená na tejto norme.

Norma ISO 22301 je štandardom pre riadenie kontinuity podnikania. Pre školy to znamená byť pripravené na narušenia: kybernetický útok, zlyhanie systému, incident ransomvéru, ktorý zablokuje prístup k záznamom študentov. Norma ISO 22301 nabáda organizácie, aby tieto situácie vopred plánovali, aby mali zavedené zálohy a postupy obnovy a aby ich pravidelne testovali, aby fungovali v prípade potreby. Škola, ktorá dodržiava tento prístup, sa môže z incidentu rýchlo zotaviť, namiesto toho, aby čelila týždňom narušenia. Časť 3.2 a postup reakcie na incidenty v dodatku IV odrážajú túto normu.

Norma ISO 31000 je štandardom pre riadenie rizík. Poskytuje spôsob uvažovania o riziku, ktorý sa vzťahuje na všetky oblasti školského života, nielen na kybernetickú bezpečnosť. Pred prijatím novej digitálnej platformy, pred zavedením nástroja umelej inteligencie, pred zmenou spôsobu nakladania s údajmi študentov by si škola mala položiť otázku: čo by sa mohlo pokaziť, aká je pravdepodobnosť a aké by boli následky? Toto je myslenie, ktoré je základom procesu DPIA v dodatku V, prístupu k hodnoteniu platformy v časti 3.3 a širšieho prístupu zameraného na uvedomenie si rizík v celej časti 3.

Týchto päť štandardov spolu tvorí chrbticu 3. časti. Sú dôvodom, prečo odporúčania v tejto politike nie sú svojvoľné. Predstavujú desaťročia nahromadených vedomostí o tom, ako môžu organizácie chrániť svoje informácie, riadiť svoje riziká a pokračovať v prevádzke, keď sa niečo pokazí. Nasledujúce usmernenia premieňajú tieto vedomosti na praktické kroky, ktoré môže podniknúť každá škola.

Časť 3: Čo by mala vaša škola urobiť

Táto časť je rozdelená do siedmich oblastí. Každá oblasť začína krátkym vysvetlením, prečo je dôležitá, po ktorom nasleduje tabuľka, ktorá ukazuje, čo musí vaša škola urobiť, prečo je každé opatrenie dôležité a ako ho vykonať.

Odporúčania v tejto časti sú najúčinnejšie, keď zahŕňajú celú školskú komunitu. Vedúci pracovníci škôl, učitelia, administratívni pracovníci, študenti, rodičia a externé podporné organizácie zohrávajú úlohu pri vytváraní bezpečného digitálneho prostredia. Pravidelná komunikácia, praktické vzdelávanie a dôveryhodné kanály nahlasovania pomáhajú školám budovať kultúru kybernetickej odolnosti, a nie len reagovať na incidenty.

3.1 Ochrana osobných údajov

Školy uchovávajú veľké množstvo osobných údajov o študentoch, rodičoch a zamestnancoch. Patria sem mená, čísla preukazov totožnosti, záznamy o dochádzke, známky, zdravotné informácie a kontaktné údaje rodiny. Ochrana týchto údajov je zákonnou povinnosťou. Je to tiež otázka dôvery. Rodiny zdieľajú citlivé informácie so školami, pretože musia. Školy majú zodpovednosť s nimi zaobchádzať opatrne.

Keď sa ochrana údajov pokazí, následky môžu byť vážne. Informácie o študentoch sa môžu dostať k ľuďom, ktorí by ich nemali mať. Škola môže čeliť formálnemu vyšetrovaniu. A dôveru študentov a rodín môže byť ťažké obnoviť. Správne nastavenie základov od začiatku je oveľa jednoduchšie ako riešenie následkov narušenia bezpečnosti.

Čo	Prečo je to dôležité	Ako to urobiť
Vymenujte zodpovednú osobu (DPO)	Zodpovedná osoba (DPO) je osoba zodpovedná za to, aby vaša škola dodržiavala zákon o ochrane údajov. Bez nej neexistuje jasná zodpovednosť, keď sa niečo pokazí. Zodpovedná osoba je tiež hlavným kontaktom pre študentov, rodičov a národný dozorný orgán.	V 2. časti zistite, či vaša škola potrebuje vlastnú zodpovednú osobu (DPO), alebo či je táto úloha zabezpečená na úrovni klastra alebo úradu. Zodpovedná osoba musí byť dostupná pre zamestnancov, študentov a rodičov. Je zodpovedná za monitorovanie dodržiavania predpisov, poradenstvo v otázkach ochrany údajov, školenie zamestnancov a spoluprácu s dozorným orgánom.
Uchovávajte záznamy o všetkých činnostiach spracovania údajov	Tento záznam je vyžadovaný zákonom podľa článku 30 GDPR. Ukazuje, aké osobné údaje vaša škola uchováva, prečo ich uchováva, kto k nim má prístup a ako dlho sa uchovávajú. Ak si ho dozorný orgán vyžiada, musíte ho byť schopní predložiť.	Register musí zahŕňať každú kategóriu osobných údajov, ktoré vaša škola spracováva: záznamy o študentoch, kontakty na rodičov, údaje o zamestnancoch, zdravotné informácie atď. Pre každú kategóriu zaznamenajte účel, právny základ, kto má prístup, ako dlho sa údaje uchovávajú a čo sa stane, keď už nie sú potrebné. Za ich aktualizáciu je zodpovedná zodpovedná osoba.
Zbierajte iba údaje, ktoré skutočne potrebujete	Každý údaj, ktorý zhromaždíte, predstavuje riziko. V prípade narušenia bezpečnosti môžu byť odhalené iba údaje, ktoré skutočne máte v držbe. Zhromažďovanie väčšieho množstva údajov, ako potrebujete, tiež znamená viac práce pri správe a väčší	Prejdite si všetky formuláre na zber údajov, procesy zápisu a nastavenia platformy. Odstráňte všetky polia, ktoré požadujú informácie, ktoré škola skutočne nepotrebuje. Ak platforma požaduje viac údajov, ako je potrebné, zatlačte na dodávateľa alebo si vyberte inú platformu. Nastavte si pravidlo, že voliteľný zber údajov je štandardne vypnutý.

Čo	Prečo je to dôležité	Ako to urobiť
	potenciál pre nedodržiavanie predpisov.	
Podpíšte zmluvy s každým dodávateľom, ktorý spracováva údaje študentov	Keď spoločnosť spracováva údaje študentov alebo zamestnancov vo vašom mene, napríklad cloudová platforma, nástroj na hodnotenie alebo komunikačná aplikácia, vaša škola zostáva právne zodpovedná za to, ako sa s týmito údajmi nakladá. Bez písomnej dohody nemôžete preukázať, že ste si splnili svoje povinnosti.	Predtým, ako akýkoľvek dodávateľ spustí službu, ktorá zahŕňa osobné údaje, musí podpísať zmluvu o spracovaní údajov. Táto zmluva musí špecifikovať, aké údaje sa spracovávajú, na aký účel, aké bezpečnostné opatrenia sa uplatňujú a čo sa s údajmi stane po skončení zmluvy. Uschovajte si kópie všetkých zmlúv.
Obmedziť, kto má prístup k osobným údajom	Čím viac ľudí má prístup k údajom, tým väčšie je riziko ich zneužitia, náhodného zverejnenia alebo krádeže. Každý nepotrebný prístupový bod je zraniteľnosťou.	Nastavte prístup založený na rolách tak, aby každý zamestnanec videl iba údaje, ktoré potrebuje pre svoju konkrétnu prácu. Učiteľ by mal vidieť záznamy svojich vlastných študentov, nie záznamy celej školy. Administratívni zamestnanci by mali mať prístup k administratívnym údajom, nie k zdravotným alebo psychologickým záznamom. Skontrolujte, kto má prístup, aspoň raz ročne a okamžite ho odstráňte, keď niekto zmení rolu alebo odíde.
Povedzte študentom a rodičom, ako sa používajú ich údaje	Študenti a rodičia majú zákonné právo vedieť, aké údaje sa o nich uchovávajú a ako sa používajú. Poskytovanie týchto informácií nie je dobrovoľné. Školy, ktoré sú transparentné, pokiaľ ide o používanie údajov, majú tiež tendenciu mať menej sporov a sťažností.	Napíšte oznámenie o ochrane osobných údajov v zrozumiteľnom jazyku, ktorému rozumie každý rodič alebo starší študent. Musí vysvetliť, aké údaje sa zhromažďujú, prečo, kto k nim má prístup a ako dlho sa uchovávajú. Poskytnite ho pri zápise študentov a vždy, keď sa niečo významne zmení. Sprístupnite ho trvalo, napríklad na webovej stránke školy. Vzorový list je v prílohe II.
Získajte súhlas rodičov pre študentov, ktorí nedosiahli vek digitálneho súhlasu	Študentov, ktorí nedosiahli národný vek digitálneho súhlasu, nemôžete zapísať na digitálnu platformu bez písomného súhlasu rodiča alebo zákonného zástupcu. Ide o zákonnú požiadavku. Vek sa v piatich krajinách pohybuje od 13 do 16 rokov, čo znamená, že tá istá platforma môže	Stanovte jasný proces zhromažďovania, zaznamenávania a obnovovania súhlasu rodičov. Súhlas musí byť špecifický pre každú platformu, udelený slobodne a ľahko odvolateľný. Nepredpokladajte, že podpísanie všeobecného registračného formulára sa vzťahuje na všetky digitálne platformy. V časti 2 si overte vek digitálneho súhlasu pre vašu krajinu.

Čo	Prečo je to dôležité	Ako to urobiť
	vyžadovať súhlas v jednej krajine, ale v inej nie.	
Nahláste úniky údajov do 72 hodín	72-hodinová lehota je prísna zákonná požiadavka. Ak vaša škola zistí porušenie a nenahlási ho včas alebo sa ho pokúsi riešiť potichu bez toho, aby informovala dozorný orgán, následky môžu byť oveľa horšie, ako keby bolo porušenie nahlásené okamžite.	Predtým, ako sa čokoľvek stane, zaveďte písomný postup reakcie na porušenie. Keď dôjde k porušeniu, zodpovedná osoba musí okamžite posúdiť, či predstavuje riziko pre jednotlivcov. Ak áno, musí byť do 72 hodín informovaný národný dozorný orgán. Ak je riziko vysoké, musia byť priamo informované aj dotknuté osoby. Na zaznamenanie každého kroku použite záznam o incidentoch v dodatku IV.

Čo je to porušenie údajov?

Porušenie ochrany údajov je akýkoľvek incident, ktorý má za následok náhodnú alebo nezákonnú stratu, zničenie, zmenu, zverejnenie alebo prístup k osobným údajom niekomu, kto by ich nemal mať. Patria sem strata USB kľúča so záznamami študentov, e-mail odoslaný nesprávnej osobe, útok ransomvéru, ktorý uzamkne školské údaje, alebo nastavenie platformy, ktoré náhodne sprístupní záznamy študentov verejnosti. Mnohé z najčastejších porušení v školách sú spôsobené ľudskou chybou, nie externými útokmi.

3.2 Zabezpečenie školských systémov

Kybernetická bezpečnosť znamená ochranu počítačov, sietí a údajov vašej školy pred útokmi a neoprávneným prístupom. Školy sú atraktívnym cieľom pre kybernetických zločincov, pretože uchovávajú citlivé údaje o deťoch a často majú obmedzené bezpečnostné zdroje. Úspešný útok môže vypnúť školské systémy, odhaliť záznamy študentov, narušiť vyučovanie na celé týždne a spôsobiť trvalé poškodenie reputácie školy.

Dobrou správou je, že väčšina úspešných kybernetických útokov zneužíva jednoduché slabiny, ktoré sa dajú opraviť bez odborných znalostí alebo veľkých rozpočtov. Za väčšinou incidentov stoja slabé heslá, neaktualizovaný softvér, zamestnanci, ktorí nerozpoznajú phishingové e-maily, a chýbajúce zálohy. Oprava týchto základných problémov má obrovský význam.

Rovnako dôležitá je príprava na okamih, keď sa niečo pokazí. Mať otestovanú zálohu a jasný postup obnovy znamená rozdiel medzi narušením, ktoré trvá niekoľko hodín, a narušením, ktoré trvá týždne. Toto je myšlienka, ktorá stojí za plánovaním kontinuity podnikania: nielen predchádzať incidentom, ale zabezpečiť, aby škola mohla naďalej fungovať a rýchlo sa zotaviť, keď k nim dôjde.

Čo	Prečo je to dôležité	Ako to urobiť
Používajte silné heslá a	Slabé heslá sú najbežnejším spôsobom, akým sa útočníci	Všetky účty zamestnancov musia používať silné heslá s dĺžkou najmenej 12 znakov, ktoré

Čo	Prečo je to dôležité	Ako to urobiť
viacfaktorové overovanie	dostávajú do školských systémov. Heslo, ktoré sa dá ľahko uhádnuť alebo ktoré sa používa na viacerých účtoch, znamená, že jedno ukradnuté heslo môže útočníkovi poskytnúť prístup ku všetkému. Viacfaktorové overovanie pridáva druhú kontrolu, ktorá chráni účty aj v prípade krádeže hesla.	kombinujú písmená, čísla a symboly. Heslá sa musia zmeniť, ak existuje dôvod domnievať sa, že boli napadnuté. Pre všetky systémy, ktoré uchovávajú údaje študentov, musí byť zapnuté viacfaktorové overovanie. Po zadaní hesla musí zamestnanec potvrdiť svoju totožnosť druhou metódou, napríklad kódom odoslaným na jeho telefón.
Udržiavajte všetok softvér a zariadenia aktuálne	Aktualizácie softvéru často obsahujú opravy bezpečnostných slabín, ktoré útočníci aktívne zneužívajú. Mnohé z najhorších útokov ransomvéru na školy boli zamerané na systémy so starým softvérom, ktorý nebol aktualizovaný. Toto je jedna z najzraniteľnejších zraniteľností, ktorej sa dá najlepšie predísť.	Nastavte pravidelný harmonogram pre aplikáciu aktualizácií na všetky školské zariadenia, operačné systémy, aplikácie a bezpečnostný softvér. Aplikujte kritické bezpečnostné záplaty hneď, ako sú k dispozícii. Ak zariadenie už nedokáže prijímať aktualizácie, odstráňte ho zo siete alebo ho vymeňte. Priraďte konkrétnemu členovi personálu zodpovednosť za zabezpečenie aktualizácií.
Pravidelne zálohujte všetky dôležité údaje	Útoky ransomvéru fungujú tak, že šifrujú vaše údaje a požadujú platbu za obnovenie prístupu. Jediným spoľahlivým spôsobom obnovenia bez platenia je mať zálohu, ktorá bola vytvorená pred útokom. Bez testovanej zálohy môže škola prísť o týždne práce a trvalé záznamy.	Nastavte automatické denné zálohy všetkých kritických školských údajov. Uchovávajte aspoň jednu kópiu každej zálohy na mieste, ktoré nie je pripojené k hlavnej sieti školy, aby nemohlo dôjsť k jej zašifrovaniu pri rovnakom útoku. Proces obnovy otestujte aspoň raz ročne, aby ste sa uistili, že zálohy skutočne fungujú a že údaje je možné obnoviť v primeranom čase.
Používajte samostatné siete pre administratívu a študentov	Ak je sieť používaná administratívnym personálom, kde sa spravujú záznamy a známky študentov, rovnaká ako sieť používaná študentmi a návštevníkmi, potom by sa napadnuté zariadenie študenta alebo infikovaný notebook návštevníka mohol potenciálne dostať do administratívnych systémov	Nastavte samostatné siete Wi-Fi: jednu pre administratívne použitie a jednu pre študentov a návštevníkov. Uistite sa, že administratívna sieť nie je viditeľná alebo dostupná zo študentskej siete. Nastavte riadenie prístupu tak, aby sa k administratívnej sieti mohli pripojiť iba autorizované školské zariadenia.

Čo	Prečo je to dôležité	Ako to urobiť
	školy. Toto je základné riziko, ktoré oddelenie siete eliminuje.	
Chráňte všetky školské zariadenia	Zariadenia, ktoré majú predvolené továrenské heslá, nikdy neboli aktualizované alebo nemajú nainštalovanú antivírusovú ochranu, sú ľahkým cieľom. Mnohé školy majú v triedach alebo kanceláriách zariadenia, ktoré boli nastavené pred rokmi a odvtedy neboli skontrolované.	Nainštalujte antivírusový a antimalvérový softvér na všetky školské zariadenia a udržiavajte ho aktualizovaný. Zmeňte všetky predvolené heslá na smerovačoch, kamerách, tlačiarňach a všetkých ostatných pripojených zariadeniach hneď po ich nainštalovaní. Vykonávajte pravidelný audit všetkých pripojených zariadení. Pred likvidáciou starých zariadení sa uistite, že všetky údaje boli natrvalo a bezpečne odstránené.
Majte písomný plán na riešenie incidentov	Bez písomného plánu zamestnanci, ktorí sa ocitnú v situácii, keď čelia kybernetickému útoku, nebudú vedieť, čo majú robiť. Panikárenie alebo dobre mienené, ale nesprávne rozhodnutia, ako napríklad okamžité vypnutie zariadenia alebo pokus o zaplatenie výkupného, môžu zlú situáciu ešte zhoršiť.	Vypracujte postup reakcie na kybernetický incident, ktorý stanoví, kto koordinuje reakciu, aké kroky podniknúť a v akom poradí, ktoré vnútroštátne orgány kontaktovať a v akom časovom rámci a ako komunikovať so študentmi, rodičmi a zamestnancami počas incidentu a po ňom. Uistite sa, že všetci zodpovední zamestnanci poznajú postup ešte predtým, ako k incidentu dôjde. Šablóna je uvedená v dodatku IV.
Školiť všetkých zamestnancov aspoň raz ročne	Phishingové e-maily stoja za väčšinou úspešných kybernetických útokov na školy. Zamestnanec, ktorý nedokáže rozpoznať phishingový e-mail, je zraniteľnosťou, pred ktorou ho žiadny technický systém nedokáže úplne ochrániť. Jedno kliknutie na škodlivý odkaz môže útočníkovi poskytnúť plný prístup k školským systémom.	Zabezpečte povinné každoročné školenie o kybernetickej bezpečnosti pre všetkých zamestnancov. Školenie musí zahŕňať, ako rozpoznať phishingový e-mail, ako vytvárať a spravovať silné heslá, čo robiť v prípade straty alebo krádeže zariadenia a na koho sa obrátiť, ak sa niečo zdá byť v neporiadku. Pridávajte pravidelné pripomienky počas celého roka. Ak je to možné, vykonávajte simulované phishingové cvičenia: tie sú jedným z najúčinnejších spôsobov, ako zmeniť správanie zamestnancov.

Čo je to phishingový útok?

Phishing je, keď útočník odošle e-mail, správu alebo oznámenie, ktoré vyzerá, akoby pochádzalo od niekoho dôveryhodného, napríklad od ministerstva školstva, poskytovateľa softvéru alebo kolegu. Cieľom je prinútiť príjemcu kliknúť na škodlivý odkaz, zadať svoje prihlasovacie údaje na

falošnej webovej stránke alebo otvoriť infikovaný súbor. Phishing je najbežnejšou formou kybernetického útoku na školy. Akákoľvek neočakávaná správa, ktorá žiada o heslo, žiada niekoho o urgentné kliknutie na odkaz alebo žiada o vykonanie nezvyčajnej akcie, by sa mala považovať za podozrievavú a overiť prostredníctvom samostatného kanála predtým, ako niekto zareaguje.

3.3 Bezpečný výber a používanie digitálnych platforiem

Školy využívajú čoraz viac digitálnych platforiem na výučbu, komunikáciu a administratívu. Každá platforma, ktorá spracováva údaje o študentoch, je potenciálnym zdrojom rizika. Platforma, ktorá má slabé zabezpečenie, zdieľa údaje s inzerentmi alebo uchováva informácie o študentoch mimo EÚ bez riadnych záruk, môže spôsobiť skutočnú škodu. Školy majú zákonnú povinnosť skontrolovať platformy pred ich prijatím a po ich použití ich starostlivo spravovať.

To isté platí pre nástroje umelej inteligencie. UI je čoraz viac prítomná vo vzdelávaní, ale nie všetky nástroje sú bezpečné na používanie so študentmi. Zákon EÚ o umelej inteligencii stanovuje jasné hranice a školy musia vedieť, kde sú tieto hranice predtým, ako zavedú akýkoľvek nástroj umelej inteligencie do triedy alebo do procesov, ktoré ovplyvňujú študentov.

Čo	Prečo je to dôležité	Ako to urobiť
Pred použitím skontrolujte každú platformu	Platforma, ktorá je prijatá bez riadnych kontrol, môže spracovávať údaje študentov spôsobmi, s ktorými škola nesúhlasila, ukladať údaje mimo EÚ alebo mať bezpečnostné nedostatky. Keď sú údaje zdieľané s nesprávnym poskytovateľom, je veľmi ťažké to vrátiť späť.	Pred prijatím akejkoľvek novej platformy overte, či je v súlade s GDPR, či nepoužíva údaje študentov na reklamu ani ich nezdieľa s tretími stranami bez súhlasu a či uchováva údaje v rámci EÚ. Ak platforma zahŕňa rozsiahle spracovanie údajov študentov, pred spustením vykonajte posúdenie vplyvu na ochranu údajov (pozri dodatok V). Pred zdieľaním akýchkoľvek údajov podpíšte s poskytovateľom zmluvu o spracovaní údajov.
Uchovávajte si zoznam schválených platforiem	Bez centrálneho záznamu školy strácajú prehľad o tom, aké platformy sa používajú, kedy boli naposledy skontrolované alebo kto ich schválil. Zamestnanci môžu začať používať platformy neformálne bez akéhokoľvek hodnotenia. Študenti môžu na školské účely používať osobné účty na neschválených nástrojoch, čím sa údaje dostanú mimo kontroly školy.	Veďte písomný register všetkých digitálnych platforiem a nástrojov schválených na používanie vo vašej škole. Zaznamenajte si názov platformy, na čo sa používa, kedy bola posúdená a kedy je plánované ďalšie preskúmanie. Register skontrolujte aspoň raz ročne. Zamestnanci nesmú zavádzať nové platformy na používanie v škole bez toho, aby najprv absolvovali proces schvaľovania.

Čo	Prečo je to dôležité	Ako to urobiť
Bezpečné nastavenie platforiem	Predvolené nastavenia na platformách sú zvyčajne navrhnuté pre jednoduché používanie, nie pre bezpečnosť. Virtuálna učebňa, ku ktorej sa môže pripojiť ktokoľvek bez prihlásenia, funkcia nahrávania, ktorá je predvolene zapnutá, alebo študentské účty s nadmerným počtom oprávnení vytvárajú riziká, ktorým sa dá ľahko vyhnúť.	Každá platforma musí byť bezpečne nakonfigurovaná predtým, ako ju študenti alebo zamestnanci začnú používať. Nástroje na videokonferencie musia vyžadovať prihlásenie predtým, ako sa ktokoľvek môže pripojiť k virtuálnej učebni. Nahrávanie musí byť štandardne vypnuté a zapnuté iba s výslovným súhlasom všetkých prítomných. Študentské účty by mali mať iba povolenia, ktoré potrebujú pre svoje vzdelávacie aktivity. Nastavenia skontrolujte aspoň raz ročne.
Zistite, ktoré spôsoby použitia umelej inteligencie sú zakázané	Niektoré postupy umelej inteligencie vo vzdelávacích prostrediach sú zakázané právnymi predpismi EÚ. Platí to bez ohľadu na to, ako bol nástroj propagovaný alebo čo predajca tvrdí. Zákaz je absolútny a vzťahuje sa na všetky školy vo všetkých piatich krajinách.	Nepoužívajte žiadny nástroj umelej inteligencie, ktorý zahŕňa rozpoznávanie emócií študentov, ich biometrickú kategorizáciu alebo ich identifikáciu v reálnom čase prostredníctvom rozpoznávania tváre. Toto použitie je zakázané podľa článku 5 zákona EÚ o umelej inteligencii. Ak dodávateľ ponúka tieto funkcie, škola ich nesmie používať. Ak škola už takýto nástroj používa, musí s ním prestať.
Nechajte ľudí zodpovedných za rozhodnutia týkajúce sa študentov	Nástroje umelej inteligencie môžu vytvárať nesprávne, zaujaté alebo nespravodlivé odporúčania. Keď tieto odporúčania ovplyvnia to, čo sa so študentom stane, napríklad známku, odporúčanie alebo posúdenie vzdelávacích potrieb, následky môžu byť vážne. Práve z tohto dôvodu zákon vyžaduje, aby za to bol zodpovedný človek.	Učiteľ alebo zodpovedná dospelá osoba musí vždy skontrolovať a prevziať zodpovednosť za akýkoľvek výstup z nástroja umelej inteligencie, ktorý ovplyvňuje študenta. Nástroje umelej inteligencie môžu pomôcť, ale nemôžu robiť konečné rozhodnutia. Zdokumentujte, ako sa uplatňuje ľudský dohľad nad každým nástrojom umelej inteligencie, ktorý sa používa pri rozhodovaní vo vzdelávaní.
Informujte študentov a rodičov o používaní umelej inteligencie	Študenti a rodičia majú právo vedieť, kedy sa nástroje umelej inteligencie používajú spôsobom, ktorý	Ak sa nástroj umelej inteligencie používa spôsobom, ktorý ovplyvňuje učenie alebo hodnotenie študenta, informujte študentov a rodičov jasne a zrozumiteľne: čo nástroj robí, aké údaje používa, ako sa používajú

Čo	Prečo je to dôležité	Ako to urobiť
	ovplyvňuje vzdelávanie študentov. Používanie nástrojov umelej inteligencie bez ich informovania pravdepodobne predstavuje porušenie zákona o umelej inteligencii aj GDPR.	jeho výstupy a ako funguje ľudský dohľad. Tieto informácie poskytnite pred použitím nástroja a uchovávajte ich trvalo prístupné.
Veďte si záznamy o všetkých používaných nástrojoch umelej inteligencie	Školy, ktoré nevedia, aké nástroje umelej inteligencie používajú, aké údaje tieto nástroje spracovávajú alebo aké hodnotenie bolo vykonané pred ich prijatím, si nemôžu splniť svoje zákonné povinnosti vyplývajúce zo zákona o umelej inteligencii alebo GDPR.	Ako súčasť zoznamu schválených platforiem si vedte register nástrojov umelej inteligencie. Pre každý nástroj umelej inteligencie zaznamenávajte, čo robí, do akej kategórie rizika patrí podľa zákona o umelej inteligencii, aké údaje spracováva, aké posúdenie bolo vykonané pred prijatím a kto je zodpovedný za dohľad. Tento záznam kontrolujte aspoň raz ročne.

3.4 Správa mobilných telefónov a osobných zariadení

Všetkých päť partnerských krajín zaviedlo právne obmedzenia týkajúce sa používania mobilných telefónov v školách. Konkrétne pravidlá sa v jednotlivých krajinách líšia (pozri 2. časť), ale dôvody sú všade rovnaké: telefóny v triedach odvádzajú pozornosť študentov od učenia, vytvárajú riziká pre súkromie a ochranu údajov, uľahčujú kyberšikanu a zvyšujú digitálny tlak, ktorý ovplyvňuje duševné zdravie študentov.

Zásady používania mobilných telefónov sú viac než len disciplinárne pravidlo. Je to opatrenie na ochranu údajov, opatrenie pre blaho študentov a vyhlásenie o tom, čo si škola cení. Zásady, ktoré sú jasne napísané, skutočne im rozumejú študenti, rodičia a zamestnanci a ktoré sa dôsledne uplatňujú, sú oveľa účinnejšie ako tie, ktoré existujú len na papieri.

Čo	Prečo na tom záleží	Ako to urobiť
Majte jasné a písomné zásady používania mobilných telefónov	Bez písomných zásad pravidlá uplatňujú rôzni učitelia rôzne. Študenti a rodičia nemôžu byť nútení dodržiavať pravidlá, o ktorých neboli jasne informovaní. Nekonzistentné presadzovanie vytvára	Vypracujte pravidlá používania mobilných telefónov, ktoré upravujú, kedy sa telefóny môžu a nesmú používať, kde sa musia uchovávať počas obmedzených časov, aké existujú výnimky pre lekárske potreby alebo špecifické vzdelávacie aktivity a čo sa stane, ak sa pravidlá porušia. Zdieľajte tieto pravidlá so študentmi a rodičmi na začiatku každého školského roka prostredníctvom

Čo	Prečo na tom záleží	Ako to urobiť
	konflikty a podkopáva dôveru v školské pravidlá.	Zásad prijateľného používania (Dodatok III). Zahrňte ich do interných predpisov školy.
Obmedzte používanie telefónu počas vyučovania	Neobmedzené používanie telefónov počas vyučovania narúša učenie, vytvára príležitosti na kyberšikanu a neoprávnené nahrávanie a zvyšuje digitálny tlak, ktorý ovplyvňuje blaho študentov. Výskum opakovane ukazuje, že študenti v školách s jasnými obmedzeniami používania telefónov dosahujú lepšie akademické výsledky a hlásia vyššiu blahobyt.	Študenti nesmú používať osobné mobilné telefóny počas vyučovania, pokiaľ im to učiteľ výslovne nepovolil pre konkrétnu vzdelávaciu činnosť. V krajinách, kde existuje zákonný zákaz, sa musí tento zákaz presadzovať. Jasne uveďte, kde musia byť telefóny uložené počas obmedzených časov. Výnimky zo zdravotných dôvodov musia byť zdokumentované.
Zakázať neoprávnené nahrávanie	Neoprávnené nahrávky študentov, učiteľov alebo iných zamestnancov predstavujú vážne porušenie súkromia a môžu byť podľa vnútroštátneho práva trestným činom. Nahrávky zdieľané online môžu spôsobiť trvalé škody zúčastneným osobám a škole. Popularita platforiem s krátkymi videami z toho robí rastúce riziko.	Jasne dajte študentom a zamestnancom najavo, že nahrávanie kohokoľvek v škole bez ich výslovného súhlasu je zakázané, či už počas vyučovania, na chodbách, na výletoch alebo na podujatiach. Jasne uveďte dôsledky. Akékoľvek neoprávnené nahrávanie, ktoré sa týka študentov alebo zamestnancov, považujte za závažný disciplinárny priestupok a v prípade potreby ho postúpte príslušným orgánom.
Uplatňujte bezpečnostné štandardy na osobné zariadenia používané na školské účely	Keď učiteľ používa osobné zariadenie na prístup k školským systémom, ochrana údajov školy je len taká silná, ako je silný najslabší článok. Osobné zariadenie so slabým heslom, zastaraným softvérom alebo lokálne uloženými údajmi o študentoch predstavuje skutočnú zraniteľnosť.	Zamestnanci, ktorí používajú osobné zariadenia na školské účely, ich musia chrániť silným heslom alebo PIN kódom, udržiavať si aktualizovaný softvér, používať zabezpečené pripojenie pri práci na diaľku a neukladať údaje študentov lokálne na osobných zariadeniach. Poskytnite zamestnancom jasné pokyny o tom, čo sa od nich očakáva.

3.5 Prevencia a reakcia na kyberšikanu

Kyberšikana je šikanovanie, ku ktorému dochádza prostredníctvom digitálnych zariadení a platforiem. Zahŕňa posielanie výhražných alebo ponižujúcich správ, zdieľanie súkromných obrázkov bez súhlasu, šírenie nepravdivých informácií online a úmyselné vylučovanie niekoho z online skupín. Kyberšikana môže spôsobiť vážne a dlhodobé poškodenie duševného zdravia, akademického výkonu a sociálnych vzťahov študentov.

Školy majú zákonnú povinnosť aj povinnosť starostlivosti predchádzať kyberšikane a reagovať, keď k nej dôjde. Kyberšikana sa nekončí pred školskou bránou. To, čo sa deje online doma večer, môže ovplyvniť skúsenosti študenta v škole nasledujúce ráno a naopak. Školy musia brať kyberšikanu rovnako vážne ako fyzické šikanovanie, a to aj vtedy, keď sa deje mimo vyučovania.

Čo	Prečo na tom záleží	Ako to urobiť
Zahrňte kyberšikanu explicitne do svojich pravidiel proti šikanovaniu	Všeobecná politika proti šikanovaniu, ktorá sa nezmieňuje o kyberšikane, necháva priestor na pochybnosti o tom, či je online správanie zahrnuté. Študenti, ktorí sú šikanovaní online, to nemusia nahlásiť, pretože si myslia, že škola povie, že to nie je ich problém.	Aktualizujte svoju politiku boja proti šikanovaniu tak, aby obsahovala samostatnú časť o kyberšikane. Mala by definovať, čo je kyberšikana, jasne uvádzať, že sa s ňou zaobchádza rovnako vážne ako s fyzickou šikanovaním, a potvrdzovať, že sa politika vzťahuje na online správanie mimo vyučovania, keď priamo ovplyvňuje školskú komunitu. Prehodnoťte politiku aspoň raz ročne.
Poučte študentov o kyberšikane	Študenti, ktorí chápu, čo je kyberšikana, prečo spôsobuje ujmu a čo robiť, keď ju vidia, s väčšou pravdepodobnosťou ju nahlásia a s väčšou pravdepodobnosťou podporia rovesníka, ktorý je terčom šikany. Naučiť študentov byť aktívnymi a podpornými okoloidúcimi je jedným z najúčinnejších prístupov.	Poskytujte veku primerané vzdelávanie o kyberšikane ako pravidelnú súčasť učebných osnov, nie ako jednorazovú udalosť. Zahrňte, ako kyberšikana vyzerá na rôznych platformách, akú škodu spôsobuje, ako podporiť niekoho, kto je terčom šikany, a ako ju nahlásiť. Zapojte študentov do formovania obsahu: viac sa zapájajú do správ, ktoré pomohli vytvoriť.
Poskytnite študentom jasný a bezpečný spôsob hlásenia	Mnoho študentov, ktorí sú obeťami kyberšikany, to nenahlási. Obávajú sa, že im nikto neuverí, že nahlásenie situáciu zhorší alebo že stratia prístup k svojmu telefónu. Bez dôveryhodného a dostupného spôsobu	Ponúknite viacero spôsobov nahlásenia kyberšikany: dôveryhodnú dospelú osobu, anonymný formulár alebo schránku a ak je to možné, národnú platformu na nahlasovanie (pozri časť 2). Tieto možnosti aktívne propagujte počas celého školského roka, nielen v septembri. Keď študent nahlási kyberšikanu, reagujte rýchlo a dajte jasne najavo, že to beriete vážne.

Čo	Prečo na tom záleží	Ako to urobiť
	nahlásenia zostanú incidenty skryté a zhoršia sa.	
Vyškoliť všetkých zamestnancov, aby rozpoznali kyberšikanu a reagovali na ňu	Mnohí učitelia si nie sú istí, ako reagovať na kyberšikanu, najmä ak ide o platformy, ktoré nepoznajú. Neistota vedie k nekonzistentným reakciám, ktoré podkopávajú schopnosť obete aj školy efektívne zvládať incidenty.	Poskytnite všetkým zamestnancom školenie, ktoré sa bude zaoberať tým, ako rozpoznať príznaky, že študent môže zažívať kyberšikanu, aký je školský postup a aká je v ňom ich úloha, ako uchovávať dôkazy vrátane snímok obrazovky, kedy zapojiť školského poradcu, rodičov alebo externé orgány a ako študenta podporiť bez toho, aby sa situácia neúmyselne zhoršila.
Reagujte rýchlo a všetko zdokumentujte	Pomalá alebo nekonzistentná reakcia vysiela signál, že škola neberie kyberšikanu vážne. Taktiež umožňuje eskaláciu incidentov a stratu dôkazov. Školy, ktoré nevedú riadne záznamy, majú problém odhaliť vzorce alebo preukázať, že konali primerane, ak je podaná formálna sťažnosť.	Keď je nahlásený incident kyberšikany, prvoradou prioritou je bezpečnosť a blaho študenta, ktorého sa incident stal obeťou. Okamžite si zapíšte podrobnosti: dátum a čas, čo sa stalo, ktoré platformy boli zapojené, kto bol zapojený, akékoľvek zhromaždené dôkazy a všetky prijaté opatrenia. Dôsledne uplatňovajte disciplinárne konanie. V dňoch a týždňoch po incidente sa spojte so študentom, ktorého sa incident stal obeťou.
Zapojte rodičov ako partnerov	Rodičia, ktorí rozumejú kyberšikane, vedia, ako o nej hovoriť so svojimi deťmi a cítia sa spojení s prístupom školy, sú oveľa efektívnejší v prevencii incidentov aj v podpore svojich detí, keď k nim dôjde.	Na začiatku roka informujte rodičov o prístupe školy ku kyberšikane, o tom, čo robiť, ak je ich dieťa postihnuté, a ako s nimi bude škola komunikovať. Použite šablónu v dodatku II. Keď dôjde k incidentom, zapojte rodičov všetkých postihnutých žiakov v súlade so školskými postupmi.

Školy nemusia tieto výzvy riešiť samy. Deň bezpečnejšieho internetu (február) a Európsky mesiac kybernetickej bezpečnosti (október) poskytujú školám hotové informačné materiály overené na úrovni EÚ. Program EÚ s názvom Lepší internet pre deti (BIK+) a sieť centier bezpečnejšieho internetu Insafe prevádzkujú linky pomoci, nástroje nahlasovania a vzdelávacie zdroje vo všetkých piatich partnerských krajinách, z ktorých môžu školy priamo čerpať.

3.6 Podpora digitálnej pohody študentov

Študenti čelia online rizikám, ktoré presahujú rámec kyberšikany a únikov údajov. Mnohí pociťujú úzkosť, nízke sebavedomie a sociálny tlak spojený s ich digitálnym životom. Strach z toho, že o niečo prídu, tlak prezentovať online idealizovanú verziu seba samého, neustále porovnávanie s ostatnými, nadmerný čas strávený pred obrazovkou a dizajn platforiem sociálnych médií, ktoré uprednostňujú angažovanosť pred blahobytom, to všetko prispieva k problémom s duševným zdravím, ktoré postihujú značný počet mladých ľudí.

Samotné obmedzenie prístupu tieto problémy nerieši. Študentom, ktorým sa jednoducho hovorí, aby menej používali technológie, bez toho, aby im sa pomohlo pochopiť prečo alebo aby im boli poskytnuté nástroje na riadenie vlastného správania, majú tendenciu sa k nim vrátiť hneď po zrušení obmedzení. Školy, ktoré zaznamenávajú trvalú pozitívnu zmenu, sú tie, ktoré kombinujú jasné hranice s úprimným vzdelávaním založeným na dôkazoch a kultúrou, v ktorej sa študenti cítia bezpečne hovoriť o tom, čo zažívajú online.

Čo	Prečo je to dôležité	Ako to urobiť
Zahrňte digitálnu pohodu do pastoračnej starostlivosti	Študenti, ktorí majú problémy s online životom, majú problémy s celkovým duševným zdravím a sociálnymi skúsenosťami. Ak sa digitálna pohoda bude považovať za samostatnú IT tému, študenti, ktorí potrebujú podporu, môžu stratiť priestor medzi službami.	Digitálna pohoda by mala byť súčasťou širšieho programu školy zameraného na pohodu a pastoráciu. Zamestnanci, ktorí podporujú študentov pri riešení iných výziev, by mali byť pripravení poskytnúť im podporu aj v oblasti digitálnych riešení. Spôsoby odporúčania by mali byť jasné: každý učiteľ, ktorý identifikuje študenta, ktorý má problémy, by mal presne vedieť, koho má zapojiť a čo sa bude diať ďalej.
Naučte študentov zdravým digitálnym návykom	Študenti, ktorí chápu, ako sú platformy sociálnych médií navrhnuté tak, aby ich udržali v pohybe, ktorí dokážu rozlíšiť medzi upraveným online obrázkom a realitou a ktorí si vyvinuli vlastné stratégie na riadenie svojich digitálnych návykov, sú lepšie pripravení bezpečne sa orientovať v online svete.	Zaraďte vzdelávanie o digitálnej pohode ako pravidelnú súčasť učebných osnov. Naučte študentov, ako fungujú algoritmy odporúčaní a prečo často zobrazujú obsah, ktorý vyvoláva silné emócie. Diskutujte o vplyve pasívneho prehliadania sociálnych médií na náladu a sebavedomie. Pomôžte študentom rozvíjať praktické stratégie na stanovenie hraníc v oblasti vlastného používania technológií.
Uistite sa, že študenti vedia, kde môžu získať pomoc	Mnoho študentov, ktorí majú problémy s niečím online, nepožiada o pomoc, pretože nevedia, že je k dispozícii, pretože sa hanbia alebo pretože sa boja, že im niekto vezme telefón. Ak sa podpora aktívne	Pravidelne študentom pripomínajte, s kým sa môžu porozprávať, ak ich niečo online trápi. Spomeňte to na zhromaždeniach, na hodinách a v každodenných interakciách, nielen v príručke. Osoba, na ktorú sa študent obráti, nemusí byť technologický expert. Stačí, ak to bude niekto,

Čo	Prečo je to dôležité	Ako to urobiť
	nepodporuje, je pre študentov, ktorí ju najviac potrebujú, neviditeľná.	komu študent dôveruje, kto ho bude počúvať bez súdenia a spojí ho so správnou pomocou.
Nezvyšujte digitálny tlak prostredníctvom školských postupov	Školy môžu neúmyselne vytvárať rovnaký digitálny tlak, aký sa snažia znížiť. Povinné školské skupinové chaty, očakávania, že študenti budú odpovedať na správy mimo vyučovania, a verejné porovnávanie študentov online môžu vysielať neužitočné signály.	Preskúmajte, ako škola komunikuje digitálne a či niektoré z jej vlastných postupov prispievajú k digitálnemu tlaku. Vyhnite sa povinným skupinovým chatom, ktoré stierajú hranicu medzi školským a osobným časom. Neočakávajte, že študenti alebo rodičia budú odpovedať na správy mimo bežných hodín. Vyhnite sa zverejňovaniu hodnotení alebo porovnaní online.
Rozpoznať, kedy má študent problémy	Študenti, ktorí majú ťažkosti s digitálnym životom, to nemusia priamo povedať. Znaky sú často behaviorálne a ľahko sa prehliadnu, pokiaľ zamestnanci nevedia, čo hľadať.	Poskytnite zamestnancom usmernenie ohľadom príznakov, že študent môže mať problémy s digitálnym životom: nezvyčajná úzkosť z toho, že si nemôže skontrolovať telefón, výkyvy nálad po online interakciách, stiahnutie sa zo spoločenských aktivít po niečom, čo sa stalo online, úzkosť spojená s jeho vzhľadom alebo s tým, ako ho ostatní vnímajú online, neochota prísť do školy po online incidente alebo akékoľvek náznaky, že je online pod tlakom alebo je terčom útoku. Keď sa tieto príznaky objavia, zamestnanci by sa mali riadiť školským postupom pre odporúčania.

3.7 Rozmanitosť, inklúzia a digitálna rovnosť

Nie všetci študenti čelia rovnakým digitálnym rizikám alebo majú rovnaký prístup k podpore. Pohlavie, sexuálna orientácia, zdravotné postihnutie, príjem rodiny a obavy o vnímanie tela ovplyvňujú skúsenosti študentov online a ich schopnosť získať pomoc, keď sa niečo pokazí. Politika, ktorá funguje dobre pre väčšinu študentov, ale prehliada skúsenosti ostatných, nie je úplná.

Budovanie inkluzívneho prístupu k digitálnej bezpečnosti znamená aktívne premýšľať o tom, ktorí študenti sú najviac ohrození, a zabezpečiť, aby sa k nim dostali školské politiky, vzdelávacie a podporné systémy.

Čo	Prečo je to dôležité	Ako to urobiť
Explicitne sa zaoberajte online škodami založenými na pohlaví a identite	Dievčatá čelia neúmerne vysokej miere online sexuálneho obťažovania, zneužívania založeného na vizuálnom vyobrazení a kyberšikany spojenej	Aktualizovať školskú politiku proti kyberšikane tak, aby výslovne zahŕňala online obťažovanie na základe pohlavia, sexuálne obťažovanie, zdieľanie intímnych obrázkov bez súhlasu a obťažovanie na

Čo	Prečo je to dôležité	Ako to urobiť
	so svojím vzhľadom. Študenti LGBTQ+ majú výrazne vyššiu pravdepodobnosť, že zažijú online obťažovanie a v dôsledku toho budú trpieť problémami s duševným zdravím. Výskum zistil, že hlásená prevalencia kyberšikany medzi študentmi LGBTQ+ sa značne líši: od zhruba 10 % do viac ako 70 % v závislosti od kontextu a že študenti LGB hlásia kyberšikanu približne dvakrát častejšie ako ich heterosexuálni rovesníci. Výskum ukazuje, že kyberšikana štatisticky sprostredkováva veľkú časť zvýšenej úzkosti, depresie a osamelosti, ktorú hlásia študenti zo sexuálnych menšín, čo znamená, že inkluzívna prevencia je ústredným mechanizmom na ochranu duševného zdravia tejto skupiny. Politika, ktorá nepomenuje tieto špecifické formy ujmy, necháva najzraniteľnejších študentov bez primeranej ochrany.	základe sexuálnej orientácie alebo rodovej identity. Zabezpečiť školenie zamestnancov, ktoré zahŕňa tieto špecifické formy ujmy a spôsoby, ako na ne reagovať. Vytvoriť školské prostredie, v ktorom sa každý študent cíti rovnako bezpečne, aby mohol nahlásiť, čo sa mu deje.
Sprístupnite vzdelávanie o digitálnej bezpečnosti študentom so zdravotným postihnutím	Študenti so zdravotným postihnutím vrátane rozdielov v učení môžu byť zraniteľnejší voči online manipulácii a zneužívaniu. Môže byť tiež ťažšie získať prístup k vzdelávaniu v oblasti digitálnej bezpečnosti, ktoré nie je navrhnuté s ohľadom na ich potreby. Ak nemajú prístup k mechanizmom nahlasovania, v skutočnosti neexistujú.	Zabezpečte, aby sa všetko vzdelávanie v oblasti digitálnej bezpečnosti poskytovalo spôsobom, ktorý je vhodný pre študentov s rôznymi vzdelávacími potrebami. Skontrolujte, či digitálne platformy používané v škole spĺňajú štandardy prístupnosti. Zabezpečte, aby mechanizmy hlásenia boli dostupné študentom, ktorí komunikujú odlišne. Spolupracujte so zamestnancami pre špeciálne vzdelávacie potreby s cieľom identifikovať študentov, ktorí môžu potrebovať dodatočnú podporu pri porozumení a riadení online rizík.
Rozpoznať a riešiť digitálnu priepasť	Študenti z rodín s nižšími príjmami môžu mať doma obmedzený alebo nespoľahlivý prístup na internet, staršie alebo zdieľané zariadenia a menej podpory dospelých pri navigácii v online svete. Študenti používajúci zdieľané zariadenia čelia väčším rizikám pre súkromie.	Nenavrhujte digitálne aktivity ani komunikačné postupy, ktoré predpokladajú úroveň domáceho pripojenia, ktorú nemajú všetci študenti. Uvedomte si, že študenti používajúci zdieľané zariadenia čelia určitým rizikám súkromia a poskytnite im konkrétne usmernenia. Zabezpečte, aby sa

Čo	Prečo je to dôležité	Ako to urobiť
	Títo študenti tiež s menšou pravdepodobnosťou rozpoznajú alebo nahlásia problémy.	vzdelávanie v oblasti digitálnej bezpečnosti dostalo ku všetkým študentom. Identifikujte študentov, ktorí nemajú dostatočné domáce pripojenie, a riešte to prostredníctvom dostupných národných programov.
Pomôžte študentom rozvíjať kritické povedomie o vnímaní tela online	Sociálne médiá neustále vystavujú študentov upraveným, filtrovaným obrázkom, ktoré stanovujú štandardy vzhľadu, ktoré nie sú realistické. To sa spája s nižším sebavedomím a úzkosťou, najmä u dospievajúcich dievčat, a v niektorých prípadoch s poruchami príjmu potravy.	Zahrňte vzdelávanie o vnímaní tela a online vzhľade ako súčasť učebných osnov digitálnej pohody. Naučte študentov, ako sa obrázky upravujú a filtrujú pred zverejnením, a pomôžte im pochopiť, že to, čo vidia online, je skôr predstavenie ako realita. Diskutujte o tom, ako algoritmy platformy zosilňujú obsah založený na vzhľade. K tejto téme pristupujte citlivo. Niektorí študenti už môžu mať problémy. Uistite sa, že sú zavedené odporúčania na špecializovanú podporu.
Na všetky tieto pravidlá pozrite inkluzívny pohľad	Politika navrhnutá bez ohľadu na skúsenosti rôznych skupín študentov bude odrážať skúsenosti väčšiny a ostatných menej chráni. Študenti, ktorí čelia najväčším online rizikám, sú často tí, ktorých skúsenosti boli najmenej brané do úvahy.	Prejdite si každú časť týchto zásad a položte si tieto otázky: Dosahujú tieto informácie na študentov, ktorí sú najviac ohrození? Sú naše spôsoby hlásenia dostupné pre každého? Zahŕňajú naše školenia zamestnancov špecifické zraniteľnosti rôznych skupín? Zapojte študentov vrátane študentov z nedostatočne zastúpených skupín do preskúmania a zlepšovania prístupu školy k digitálnej bezpečnosti.

Časť 4: Čo ukazujú dôkazy

Táto časť sumarizuje, čo nám výskum hovorí o tom, čo skutočne funguje, keď sa školy zaoberajú kybernetickou bezpečnosťou, kyberšikanou a digitálnou pohodou. Túto časť použite na informované rozhodnutia o programoch, prístupoch a intervenciách, ktoré vaša škola prijíma.

4.1 Povedomie a školenia v oblasti kybernetickej bezpečnosti

Výskum kybernetickej bezpečnosti v školách opakovane identifikuje ľudské správanie ako najdôležitejší rizikový faktor. Väčšina úspešných útokov začína phishingovým e-mailom alebo slabým heslom. Technická obrana síce pomáha, ale nedokáže zabrániť útoku, ak zamestnanci nie sú vyškolení na rozpoznanie hrozby. To znamená, že investícia do školenia zamestnancov je prinajmenšom rovnako dôležitá ako investícia do technických nástrojov.

Štúdie o školeniach zamestnancov v oblasti kybernetickej bezpečnosti ukazujú, že pravidelné praktické školenia fungujú výrazne lepšie ako jednorazové školenie zamerané na zvýšenie povedomia. Zamestnanci, ktorí absolvujú každoročné školenie a občasné pripomienky, s merateľne menšou pravdepodobnosťou kliknú na phishingové odkazy alebo budú používať nebezpečné praktiky v školských systémoch. Dôležitý je aj spôsob, akým je školenie poskytované: interaktívne školenia s príkladmi z reálneho sveta fungujú lepšie ako pasívne čítanie informácií alebo sledovanie videa.

Simulované phishingové cvičenia, pri ktorých zamestnanci dostanú starostlivo navrhnutý falošný phishingový e-mail, aby sa otestovala ich reakcia, patria medzi najúčinnejšie dostupné tréningové metódy. Školy a organizácie, ktoré tieto cvičenia pravidelne vykonávajú, pozorujú v priebehu času zjavné zlepšenia v správaní zamestnancov. Cvičenie je najúčinnejšie, keď po ňom okamžite nasleduje spätná väzba s vysvetlením, aké boli signály a aká by bola správna reakcia.

Pre študentov dôkazy ukazujú, že vzdelávanie v oblasti kybernetickej bezpečnosti funguje najlepšie, keď je súčasťou učebných osnov, a nie je poskytované ako samostatná udalosť. Študenti, ktorí sa učia o online bezpečnosti prostredníctvom reálnych príkladov, interaktívnych aktivít a diskusií so svojimi rovesníkmi, lepšie vstrebávajú poznatky a dôslednejšie ich uplatňujú vo svojom živote ako študenti, ktorí dostávajú rovnaké informácie na prednáške.

4.2 Prevencia kyberšikany

Výskum v oblasti prevencie kyberšikany opakovane ukazuje, že najlepšie fungujú celoškolské prístupy. To znamená programy, ktoré spájajú študentov, učiteľov, rodičov a vedenie školy okolo spoločného cieľa, ktorým je vytvorenie bezpečnejšieho prostredia. Školy, ktoré berú kyberšikanu čisto ako disciplinárnu záležitosť, ktorá sa rieši po vzniku incidentov, opakovane dosahujú horšie výsledky ako školy, ktoré uplatňujú celokomunitný prístup k prevencii.

Programy, ktoré sa zameriavajú iba na správanie šikanujúcich, sú menej účinné ako tie, ktoré zároveň budujú empatiu a zručnosti prizerania sa. Študenti, ktorí chápu škody spôsobené kyberšikanou a ktorí sa naučili, ako podporiť rovesníka, ktorý je terčom šikanovania, s väčšou pravdepodobnosťou nahlásia incidenty a s väčšou pravdepodobnosťou zasiahnu a pomôžu. Či prizerajúci zasiahnu alebo zostanú ticho, je jedným z najsilnejších prediktorov toho, či sa šikanovanie stupňova alebo zastaví.

Systémy anonymného hlásenia neustále vedú k nahláseniu väčšieho počtu incidentov. Študenti, ktorí zažijú kyberšikanu, to často nikomu nepovedia, pretože sa boja, že im nikto neuverí, že sa veci zhoršia alebo že to bude mať sociálne následky medzi ich rovesníkmi. Školy, ktoré ponúkajú skutočne dôverný a dôveryhodný spôsob hlásenia, zaznamenávajú vyššiu mieru odhalenia a skoršieho zásahu.

Školenie učiteľov je nevyhnutné a často podceňované. Výskum ukazuje, že mnohí učitelia si nie sú istí, ako reagovať na kyberšikanu, najmä ak ide o aplikácie alebo funkcie, s ktorými nie sú oboznámení. Školy, ktoré investujú do praktického a štruktúrovaného školenia učiteľov v oblasti rozpoznávania a reakcie na kyberšikanu, dosahujú u študentov trvalo lepšie výsledky.

Zapojenie rodičov tiež prináša trvalý rozdiel. Rodičia, ktorí rozumejú kyberšikane, vedia, ako fungujú platformy, ktoré ich deti používajú, a cítia sa prepojení s prístupom školy, dokážu lepšie podporovať svoje deti a posilňovať posolstvá školy doma.

Výskum poskytuje jasné dôkazy o rozsahu problému. Podľa štúdie WHO o zdravotnom správaní u detí školského veku (2024) približne každý šiesty dospievajúci v Európe, čo predstavuje približne 15 %, uvádza, že zažil kyberšikanu, pričom miera výskytu je medzi chlapcami a dievčatami vo všeobecnosti podobná a v porovnaní s rokom 2018 má rastúci trend. Údaje OECD zistili rozdiely medzi krajinami v rozmedzí od približne 7,5 % do 27,1 %. Údaje o linkách pomoci zo siete EÚ Insafe konzistentne zaraďujú kyberšikanu medzi najčastejšie dôvody, prečo deti a dospievajúci kontaktujú podporné služby, a v 4. štvrťroku 2025 to bol opäť najčastejšie zdôrazňovaný problém.

Keď Európska komisia v roku 2025 konzultovala s viac ako 6 000 deťmi a tínedžermi vo veku 12 až 17 rokov z celej EÚ, vyjadrilo jasné očakávania od škôl: väčšina chcela jasné pravidlá a dôsledky za kyberšikanu, priame vyučovanie na túto tému a psychologickú podporu pre postihnutých. Dievčatá trvalo častejšie žiadali o tieto opatrenia ako chlapci.

Metaanalýza Polanina a kol. (2021), ktorá zahŕňala viac ako 45 000 študentov, zistila, že špecializované programy na prevenciu kyberšikany viedli k štatisticky významnému zníženiu páchateľstva aj viktimizácie a že programy navrhnuté špeciálne pre kyberšikanu prekonali všeobecné prístupy proti šikanovaniu.

4.3 Digitálna pohoda

Výskum o používaní technológií a duševnom zdraví študentov nepodporuje jednoduché závery. Nie každé používanie technológií je škodlivé. Aktívne používanie technológií na kreatívnu prácu, komunikáciu alebo učenie môže mať pozitívne účinky. Trvalým problémom je pasívne používanie: prechádzanie sociálnych médií bez účelu alebo zmysluplnej interakcie. Tento typ používania je najsilnejšie spojený s úzkosťou, osamelosťou a nižším sebavedomím, pričom účinky sú obzvlášť výrazné u dospievajúcich dievčat.

Dôkazy silne podporujú vzdelávanie pred obmedzovaním. Školy, ktoré sa zameriavajú výlučne na obmedzovanie prístupu k technológiám bez toho, aby pomohli študentom pochopiť, prečo sú určité vzorce používania škodlivé, alebo im poskytli nástroje na riadenie vlastného správania, zaznamenávajú menej trvalú zmenu. Študenti, ktorí problému rozumejú a vyvinuli si vlastné stratégie, vykazujú trvalejšie zlepšenie v oblasti blahobytu.

Programy, ktoré učia študentov kriticky premýšľať o svojich digitálnych návykoch, pochopiť, ako sú platformy sociálnych médií navrhnuté tak, aby maximalizovali zapojenie, a rozpoznať rozdiel medzi kurátorsky upravenými online obrázkami a realitou, preukázali pozitívne výsledky pri znižovaní úzkosti a zlepšovaní sebavedomia vo viacerých štúdiách. Tieto programy fungujú najlepšie, keď sú poskytované postupne ako súčasť učebných osnov, a nie ako jednorazová udalosť.

Dôsledné zapojenie študentov do tvorby školských digitálnych pravidiel zvyšuje mieru ich dodržiavania a pocit zodpovednosti za pravidlá. Študenti, ktorí majú pocit, že pravidlá sú spravodlivé a že mali možnosť podieľať sa na ich tvorbe, ich s väčšou pravdepodobnosťou budú dodržiavať a s väčšou pravdepodobnosťou budú povzbudzovať svojich rovesníkov, aby robili to isté.

Obzvlášť dôležité zistenie sa týka strachu z premeškania niečoho (FOMO). Výskum čoraz viac chápe FOMO nie ako prechodnú náladu, ale ako relatívne stabilnú psychologickú charakteristiku, pretrvávajúcu úzkosť z premeškania obohacujúcich zážitkov, ktoré zažívajú iní. Štúdie spájajú FOMO s depresívnymi príznakmi, poruchami spánku a kompulzívnym kontrolným správaním. Systematický prehľad a metaanalýza z roku 2025 potvrdili konzistentnú štatistickú súvislosť medzi závislosťou od sociálnych médií a vyššou úrovňou úzkosti, depresie, osamelosti a nižšieho sebavedomia, pričom FOMO sa často identifikuje ako

sprostredkujúci faktor. Školy by sa mali explicitne zaoberať FOMO a kompulzívnymi vzormi užívania v aktivitách zameraných na študentov, nielen prostredníctvom všeobecných správ o čase strávenom pred obrazovkou.

Výskum tiež poznamenáva, že výsledky vo veľkej miere závisia nielen od toho, koľko študenti používajú digitálne platformy, ale aj od toho, ako ich používajú. Sociálne médiá môžu slúžiť ako zdroj podpory pre niektorých študentov, najmä pre tých, ktorí sú izolovaní alebo patria k menšinovým skupinám. Preventívne prístupy by mali študentom pomôcť rozvíjať uvedomelejší a zámernejší vzťah k technológiám.

Včasná identifikácia a odporúčanie sú dôležité. Študenti, ktorí sú spojení so správnou podporou skôr, ako sa ich ťažkosti stanú vážnymi, dosahujú výrazne lepšie výsledky ako tí, u ktorých sú problémy identifikované až vtedy, keď sú už viditeľné prostredníctvom zhoršujúcich sa známok alebo závažných zmien v správaní. Školy, ktoré majú jasné a dobre známe spôsoby, ako odhaliť a podporiť študentov, ktorí majú problémy, sú v oveľa lepšej pozícii, aby im pomohli.

Dodatok I: Národná referenčná tabuľka

Túto tabuľku použite na vyhľadanie kľúčových národných parametrov pre vašu krajinu. Ak táto politika uvádza, že je potrebné skontrolovať národné pravidlá, hľadajte ich tu.

Parameter	Grécko	Taliansko	Portugalsko	Rumunsko	Slovensko
Vek digitálneho súhlasu	15 rokov	14 rokov	13 rokov	16 rokov	16 rokov
Úrad na ochranu údajov	HDPA dpa.gr	Záruka garanteprivacy.it	CNPD cnpd.pt	ANSPDCP ochrana údajov.ro	UOOU dataprotection.gov.sk
Úrad pre kybernetickú bezpečnosť	EAKE cyber.gov.gr	ACN acn.gov.it	CNCS cncs.gov.pt	DNSC dnsc.ro	NBU nbu.gov.sk
Hlásenie kybernetických incidentov	EAKE	ACN	CERT.PT (24 hodín pre NIS2)	DNSC/PNRISC (24 hodín)	NBU/SK-CERT
Hlásenie porušení údajov	HDPA, 72 hodín	Záruka, 72 hodín	CNPD, 72 hodín	ANSPDCP, 72 hodín	UOOU, 72 hodín
Zdroj informácií o kyberšikane	stop-bullying.gov.gr	Nahlásiť v škole alebo na polícii	seguranet.pt	Škola alebo ANSPDCP	Usmernenie 1/2025
Zákon o mobilných telefónoch	Prísny zákaz 2018/2024	Všetky cykly 2024/25	1. – 6. ročník od septembra 2025	Počas vyučovania, zákon 198/2023	Všetky stupne od januára 2025
Pokyny pre školy v oblasti umelej inteligencie	Iba zákon EÚ o umelej inteligencii	MD 166/2025	Zatiaľ nevydané	Zatiaľ nevydané	Plán umelej inteligencie na roky 2025 – 2027

Dodatok II: Vzor listu pre rodičov

Školy môžu tento list upraviť tak, aby informovali rodičov o tom, ako škola nakladá s údajmi študentov a čo robí pre zaistenie bezpečnosti študentov online. Pošlite ho pri zápise a vždy, keď dôjde k významným zmenám v digitálnych systémoch alebo politikách školy.

[Názov a adresa školy]

[Dátum]

Vážený rodič/opatrovník,

Ako chránime údaje vášho dieťaťa a podporujeme jeho digitálnu bezpečnosť

Píšeme vám, aby sme vám oznámili, ako naša škola nakladá s osobnými údajmi študentov a čo robíme pre to, aby sme vaše dieťa zaistili v jeho digitálnom vzdelávacom prostredí bezpečnosť.

Aké údaje zhromažďujeme a prečo. Zhromažďujeme osobné údaje o vašom dieťati, ktoré sú potrebné na vzdelávanie a administratívu. Patria sem jeho meno, identifikačné číslo, záznamy o dochádzke a známky. V niektorých prípadoch môžeme uchovávať aj informácie týkajúce sa zdravotného stavu, ak sú relevantné pre jeho vzdelávanie. Zhromažďujeme iba to, čo potrebujeme, a uchovávame to tak dlho, ako to vyžaduje zákon.

Kto k nim má prístup. Prístup k osobným údajom vášho dieťaťa je obmedzený na oprávnených zamestnancov, ktorí ich potrebujú na výkon svojej práce. Údaje nezdieľame s externými stranami, pokiaľ to nevyžaduje zákon alebo ste na to nedali výslovný súhlas.

Digitálne platformy. Naša škola používa digitálne platformy na výučbu a administratívu. Pred prijatím akejkoľvek platformy kontrolujeme, či je v súlade s GDPR. Vaše dieťa bude mať prístup k týmto platformám prostredníctvom školského účtu. Zoznam platforiem, ktoré v súčasnosti používame, je k dispozícii v školskej kancelárii.

Váš súhlas. V prípade študentov mladších ako [vložte národný vek digitálneho súhlasu] potrebujeme písomný súhlas rodičov predtým, ako ich budeme môcť zapísať na digitálnu platformu. O tento súhlas budete požiadaní pri zápise a vždy, keď bude zavedená nová platforma.

Kyberšikana. Naša škola má jasné postupy na prevenciu a reakciu na kyberšikanu. Ak vaše dieťa zažije alebo vidí kyberšikanu, povzbudte ho, aby sa porozprávalo s dôveryhodnou dospelou osobou v škole alebo nás kontaktovalo priamo na adrese [kontaktné údaje].

Vaše práva. Máte právo vidieť údaje, ktoré o vašom dieťati uchovávame, požiadať o ich opravu a za určitých okolností požiadať o ich vymazanie. Ak to chcete urobiť, kontaktujte nášho úradníka pre ochranu údajov na adrese [kontaktné údaje DPO].

Podpora digitálnej pohody doma. Odporúčame vám, aby ste sa so svojím dieťaťom pravidelne rozprávali o jeho online skúsenostiach bez odsudzovania. Ak sa zdá, že vaše dieťa je v úzkosti alebo nezvyčajne

úzkostlivé z telefonovania alebo online interakcií, kontaktujte, prosím, [školského poradcu / určenú kontaktnú osobu]. Pre deti a mládež sú vo vašej krajine k dispozícii aj národné linky pomoci.

Ak máte akékoľvek otázky, neváhajte nás kontaktovať.

S úctou,

[Meno riaditeľa a škola]

Dodatok III: Šablóna zásad prijateľného používania

Upravte túto šablónu a vytvorte si vlastné Zásady prijateľného používania pre vašu školu. Mali by ich podpísať študenti, rodičia alebo opatrovníci a zamestnanci na začiatku každého školského roka. Upravte ju tak, aby odrážala školské systémy, národné pravidlá a kontext vašej školy.

Zásady prijateľného používania

[Názov školy] | Akademický rok [XXXX-XXXX]

1. Účel

Tieto zásady stanovujú pravidlá používania digitálnych zariadení, internetu a digitálnych platforiem v našej škole. Vzťahujú sa na všetkých študentov, zamestnancov a návštevníkov, ktorí používajú školské systémy. Podpísaním týchto zásad potvrdzujete, že ste si tieto pravidlá prečítali a rozumiete im a súhlasíte s ich dodržiavaním.

2. Na čo môžete použiť školské digitálne zdroje

- Dokončovanie školských úloh a vzdelávacích aktivít
- Komunikácia s učiteľmi a spolužiakmi v školských záležitostiach
- Používanie platforiem, ktoré schválila škola
- Vzdelávacie aktivity, ktoré učiteľ osobitne povolil

3. Čo nesmiete robiť

- Prístup, vytváranie alebo zdieľanie obsahu, ktorý je nezákonný, škodlivý, urážlivý alebo diskriminačný
- Šikanovať, obťažovať, vyhrážať sa alebo ponižovať iných študentov alebo zamestnancov prostredníctvom digitálnych prostriedkov
- Zdieľajte osobné údaje o iných študentoch alebo zamestnancoch bez ich súhlasu
- Nahrávať video alebo audio študentov, učiteľov alebo zamestnancov bez ich výslovného súhlasu
- Používanie účtu inej osoby alebo zdieľanie svojich prihlasovacích údajov
- Inštalácia softvéru alebo aplikácií na školské zariadenia bez autorizácie
- Používajte osobné účty na neschválených platformách na školské aktivity

4. Mobilné telefóny

[Opíšte tu pravidlá používania mobilných telefónov vo vašej škole v súlade s vnútroštátnymi zákonmi vašej krajiny, ako je uvedené v časti 2 týchto pravidiel. Uveďte, kde musia byť telefóny uložené, aké výnimky platia a čo sa stane, ak sa pravidlá porušia.]

5. Sociálne médiá

Študenti nesmú uverejňovať obsah o škole, iných študentoch alebo zamestnancoch, ktorý je škodlivý, zavádzajúci alebo by mohol poškodiť reputáciu kohokoľvek. Online správanie, ktoré sa rovná kyberšikane, či už počas vyučovania alebo mimo neho, je upravené týmito zásadami a postupmi školy proti šikanovaniu.

6. Podávanie správ

Ak narazíte na obsah, ktorý vy alebo iný študent vyvoláva pocit bezpečia, alebo ak spozorujete porušenie týchto zásad, nahláste to dôveryhodnej dospelej osobe v škole alebo na adresu [kontakt pre nahlasovanie].

7. Dôsledky

Porušenie týchto zásad môže mať za následok pozastavenie prístupu do školských systémov, ďalšie disciplinárne opatrenia podľa disciplinárnych pravidiel školy a v závažných prípadoch aj postúpenie veci orgánom činným v trestnom konaní.

Celé meno študenta	
Podpis študenta	
Meno rodiča alebo zákonného zástupcu	
Podpis rodiča alebo zákonného zástupcu	
Dátum	

Dodatok IV: Postup reakcie na kybernetický incident

Vždy, keď sa vo vašej škole vyskytne kybernetický incident, postupujte podľa týchto krokov. Kybernetický incident je akákoľvek udalosť, ktorá ohrozí bezpečnosť, dostupnosť alebo dôvernosť školských údajov alebo systémov. Patria sem útok ransomvéru, neoprávnený prístup k školským systémom alebo porušenie ochrany osobných údajov.

Krok 1: Identifikujte a izolujte

Hneď ako niekto zistí incident, musí to okamžite oznámiť koordinátorovi IT alebo riaditeľovi školy. Nepokúšajte sa problém vyriešiť sami. Odpojte postihnuté zariadenie od siete odpojením kábla alebo vypnutím Wi-Fi. Nevypínajte zariadenie, pokiaľ vám to nie je výslovne nariadené, pretože by ste mohli zničiť dôkazy. Zapíšte si čas a popis toho, čo ste pozorovali.

Krok 2: Posúdenie

Koordinátor IT a zodpovedná osoba za ochranu údajov musia incident posúdiť spoločne. Zistiť, ktoré systémy, účty alebo údaje boli ovplyvnené. Zistiť, či boli alebo mohli byť osobné údaje ohrozené. Overiť, či incident stále prebieha alebo bol podaný do poriadku.

Krok 3: Upozorniť

Ak sa to stalo...	Mali by ste...
Osobné údaje boli alebo mohli byť ohrozené	Do 72 hodín o tom informujte národný orgán na ochranu údajov. Informácie o orgáne vo vašej krajine nájdete v časti 2.
Došlo k závažnému kybernetickému bezpečnostnému incidentu	Informujte národný orgán kybernetickej bezpečnosti. V Portugalsku to musia subjekty, na ktoré sa vzťahuje NIS2, urobiť do 24 hodín. Informácie o orgánoch vašej krajiny nájdete v časti 2.
Je zapojená trestná činnosť	Kontaktujte políciu.
Študenti alebo zamestnanci sú v bezprostrednom ohrození alebo im bola priamo spôsobená ujma	Okamžite poskytnite podporu a v prípade potreby informujte rodičov alebo opatrovníkov.

Krok 4: Obnova

Ak sú k dispozícii, obnovte systémy zo záloh. Okamžite resetujte všetky dotknuté heslá a prístupové údaje. Pred opätovným uvedením systémov do používania nainštalujte všetky relevantné bezpečnostné aktualizácie. Pred opätovným sprístupnením študentom a zamestnancom skontrolujte, či obnovené systémy fungujú správne.

Krok 4a: Podporte postihnutých

Poskytnite okamžitú psychologickú a praktickú podporu každému študentovi alebo zamestnancovi, ktorého sa incident priamo dotkol. Toto by sa malo diať súbežne s technickou reakciou, nie po nej.

Bezodkladne kontaktujte školského poradcu alebo tím pastoračnej starostlivosti. Dodržiavajte školský protokol o blahobyte.

Krok 5: Kontrola

Po vyriešení incidentu vykonajte jeho úplné preskúmanie. Zapíšte si, čo sa stalo, ako k tomu došlo, čo sa urobilo a aký bol výsledok. Identifikujte, aké zmeny by znížili riziko opakovania incidentu. Informujte príslušných zamestnancov o zisteniach, najmä ak incident zahŕňal phishingový e-mail alebo ľudskú chybu. V prípade potreby aktualizujte postup reakcie na incident.

Záznam incidentov

Dátum a čas incidentu	
Ako to bolo objavené a kým?	
Čo sa stalo?	
Ktoré systémy a údaje boli ovplyvnené?	
Okamžité prijaté opatrenia	
Boli osobné údaje ohrozené?	
Bol orgán na ochranu údajov informovaný? (Dátum)	
Bol orgán kybernetickej bezpečnosti informovaný? (Dátum)	
Bola kontaktovaná polícia? (Dátum)	
Prijaté opatrenia na obnovu	
Dátum obnovenia systémov	
Bola kontrola dokončená? (Dátum)	
Zmeny vykonané v dôsledku preskúmania	

Dodatok V: Šablóna posúdenia vplyvu na ochranu údajov (DPIA)

Pred zavedením nového digitálneho systému alebo platformy, ktorá zahŕňa spracovanie veľkého množstva údajov o študentoch, systematické monitorovanie študentov, automatizované rozhodovanie, ktoré ovplyvňuje študentov, alebo citlivé kategórie údajov, sa vyžaduje posúdenie vplyvu na ochranu údajov. Ak si nie ste istí, či je posúdenie vplyvu na ochranu údajov potrebné, obráťte sa na svojho zodpovedného pracovníka za ochranu údajov.

Časť A: Čo sa bude spracovávať

Názov systému alebo platformy	
Poskytovateľ alebo predajca	
Aké osobné údaje budú spracované?	
Kto sú dotknuté osoby? (študenti, zamestnanci, rodičia)	
Aký je účel spracovania?	
Aký je právny základ pre spracovanie?	
Kde budú údaje uložené? (krajina, v rámci EHP?)	
Kto bude mať prístup?	
Ako dlho budú údaje uchovávané?	
Budú údaje zdieľané s tretími stranami?	

Časť B: Posúdenie rizika

Riziko	Úroveň (nízka / stredná / vysoká) a ako sa bude riešiť
Neoprávnený prístup k údajom študentov	
Stratené alebo omylom vymazané údaje	
Údaje použité na iné účely ako pôvodné	
Študenti sú monitorovaní alebo profilovaní bez transparentnosti	

Riziko	Úroveň (nízka / stredná / vysoká) a ako sa bude riešiť
Údaje prenesené mimo EHP bez záruk	
Údaje uchovávané dlhšie, ako je potrebné	

Časť C: Rozhodnutie

Celková úroveň rizika (nízka / stredná / vysoká)	
Môže spracovanie pokračovať? (Áno / Áno so zmierňujúcimi opatreniami / Nie)	
Čo je potrebné urobiť pred začatím spracovania?	
Bola konzultovaná osoba s DPO? (Áno / Nie / Dátum)	
Hodnotenie dokončil/a	
Dátum posúdenia	
Dátum ďalšieho preskúmania	

Dodatok VI: Register rizík školy

Školský register rizík pomáha vašej škole identifikovať, posúdiť a riadiť kľúčové riziká v oblasti kybernetickej bezpečnosti a ochrany údajov, ktorým čelí. Vyplnenie tohto registra je praktickým krokom pri implementácii prístupu k riadeniu rizík opísaného v časti 3 tejto politiky.

Príklady v tabuľke nižšie sú orientačné. Sú uvedené, aby pomohli vašej škole začať a ilustrovali druhy rizík, ktoré sú v školskom prostredí najbežnejšie. Vaša škola by mala pridávať, odstraňovať alebo upravovať záznamy tak, aby odrážali jej vlastné špecifické okolnosti, systémy a kontext. Register by sa mal kontrolovať aspoň raz ročne a aktualizovať vždy, keď dôjde k významnej zmene, ako je napríklad zavedenie novej digitálnej platformy alebo kybernetický bezpečnostný incident.

Ako hodnotiť riziká

Pre každé riziko ohodnoťte pravdepodobnosť a dopad na stupnici od 1 do 5 (1 = veľmi nízke, 5 = veľmi vysoké). Vynásobte tieto dve skóre, aby ste získali skóre rizika.

Vysoké riziko (15 – 25): musí sa riešiť okamžite.

Stredne vysoké riziko (8 – 14): musí sa riešiť, uprednostniť tie s vysokým vplyvom.

Stredne nízke riziko (4 – 7): malo by sa riešiť tam, kde je vplyv významný.

Nízke riziko (1-3): prijateľné, pravidelne monitorovať.

Orientačná tabuľka registra rizík je na nasledujúcej strane (na šírku).

Identifikácia	Riziko	Čo sa môže stať	Ako to znižujeme	Pravdepodobnosť (1-5)	Dopad (1-5)	Skóre rizika	Zodpovedný	Ak sa to stane
1	Zamestnanci zameraní na phishingové e-maily	Zamestnanci kliknú na škodlivý odkaz, čím útočníkovi poskytnú prístup k školským systémom a údajom študentov	Ročné školenie zamestnancov, simulované phishingové cvičenia, viacfaktorové overovanie na všetkých účtoch	4	4	16	Riaditeľ / IT koordinátor	Izolujte postihnuté zariadenie, informujte národný orgán pre kybernetickú bezpečnosť, obnovte ho zo zálohy
2	Útok ransomvéru	Školské systémy sú uzamknuté, záznamy a známky študentov sú neprístupné	Pravidelne testované zálohy uložené offline, aktuálny antivírusový softvér, školenie zamestnancov	3	5	15	IT koordinátor	Obnoviť zo zálohy, nahlásiť to národnému orgánu kybernetickej bezpečnosti, informovať orgán na ochranu údajov, ak sú dotknuté údaje študentov
3	Údaje študenta boli omylom odoslané	Osobné údaje študenta boli omylom zdieľané s	Školenie zamestnancov o manipulácii s údajmi,	4	3	12	DPO	Kontaktujte príjemcu a požiadajte o vymazanie, v prípade potreby

Identifikácia	Riziko	Čo sa môže stať	Ako to znižujeme	Pravdepodobnosť (1-5)	Dopad (1-5)	Skóre rizika	Zodpovedný	Ak sa to stane
	nesprávnej osobe	neoprávnenou osobou	používanie iba oficiálnych komunikačných kanálov školy					nahláste incident národnému orgánu na ochranu údajov do 72 hodín a incident zdokumentujte.
4	Kyberšikana prostredníctvom školskej platformy	Študent používa školský komunikačný nástroj na obťažovanie iného študenta	Zásady prijateľného používania podpísané všetkými študentmi a rodičmi, vzdelávanie o kyberšikane, jasný postup nahlasovania	4	3	12	Riaditeľ / Triedny učiteľ	Dodržiavajte školský postup proti šikanovaniu, podporte postihnutého študenta, zapojte rodičov, zdokumentujte incident

Dodatok VII: Register mapovania údajov

Register mapovania údajov pomáha vašej škole zaznamenávať všetky osobné údaje, ktoré spracováva. Vedenie tohto registra je zákonnou požiadavkou podľa článku 30 GDPR. Musí byť na požiadanie k dispozícii národnému orgánu na ochranu údajov.

Nižšie uvedené príklady pokrývajú najbežnejšie kategórie osobných údajov spracúvaných školami. Sú len orientačné: vaša škola by mala pridať všetky ďalšie kategórie, ktoré sa vzťahujú na vašu vlastnú situáciu, a odstrániť tie, ktoré sa nevzťahujú. Register skontrolujte a aktualizujte aspoň raz ročne a vždy, keď sa zavedie nový systém alebo platforma.

Čo je právny základ?

Vždy, keď vaša škola spracúva osobné údaje, musí na to mať zákonný dôvod. Najbežnejšie dôvody pre školy sú:

Právna povinnosť: spracovanie vyžadované vnútroštátnym zákonom o vzdelávaní (napr. vedenie záznamov o dochádzke).

Verejná úloha: spracovanie potrebné na to, aby škola mohla vykonávať svoje verejné funkcie.

Súhlas: osoba súhlasila so spracovaním (vyžaduje sa pre fotografie, nepodstatné platformy).

Orientačná tabuľka registra mapovania údajov je na nasledujúcej strane (na šírku).

Typ údajov	Prečo to spracovávame	Právny základ	Kde je uložené	Kto má prístup	Ako dlho si to necháme	Zálohované?	Zdieľané s
Osobné údaje študenta (meno, občiansky preukaz, adresa, dátum narodenia)	Vyžaduje sa pre správu školy a dodržiavanie národných zákonov o vzdelávaní	Právna povinnosť	Národný školský informačný systém (napr. MySchool, SIIIR, Unica)	Riaditeľ, iba administratívny personál	V súlade s požiadavkami vnútroštátneho práva	Áno	Ministerstvo školstva prostredníctvom národnej platformy
Akademické záznamy študentov (známky, dochádzka, hodnotenia)	Povinné sledovať pokrok študenta a informovať rodičov	Právna povinnosť / Verejná úloha	Školský informačný systém a žiacka kniha učiteľov	Triedni učitelia, riaditeľ, administratívni pracovníci	V súlade s požiadavkami vnútroštátneho práva	Áno	Rodičia (prostredníctvom zabezpečeného kanála), Ministerstvo školstva
Informácie o zdravotnom stave študenta (alergie, zdravotné postihnutia, zdravotné potreby)	Nevyhnutné na ochranu zdravia a bezpečnosti študentov počas školského dňa	Právna povinnosť / Životne dôležité záujmy	Zabezpečený papierový súbor alebo šifrovaný digitálny záznam	iba riaditeľ, školská zdravotná sestra a príslušní učitelia	Trvanie zápisu plus podľa zákonných požiadaviek	Áno (šifrované)	Poskytovatelia zdravotnej starostlivosti iba v nevyhnutných prípadoch
Fotografie a obrázky študentov	Identifikačné údaje školy, publikácie, dokumentácia o podujatiach	Súhlas rodičov	Školský server alebo schválená platforma	Administratívni zamestnanci, učitelia s oprávnením	Trvanie zápisu; na požiadanie vymazané	Áno	Žiadne zdieľanie tretích strán

Typ údajov	Prečo to spracovávame	Právny základ	Kde je uložené	Kto má prístup	Ako dlho si to necháme	Zálohované?	Zdieľané s
							bez ďalšieho súhlasu

Dodatok VIII: Register školských politík a postupov

Tento register pomáha vašej škole sledovať kľúčové bezpečnostné a ochranné zásady, ktoré má zavedené. Zdokumentované zásady v každej z týchto oblastí sú dôležitým znakom toho, že škola riadi svoje zodpovednosti v oblasti kybernetickej bezpečnosti a ochrany údajov štruktúrovaným spôsobom.

Nižšie uvedené zásady sú tie, ktoré najviac súvisia s odporúčaniami v tejto politike kybernetickej odolnosti. Zoznam je len orientačný: vaša škola môže mať ďalšie zásady, ktoré by sa tu mali tiež zaznamenať. Pre každú zásadu uveďte, kto je za ňu zodpovedný, kedy bola naposledy aktualizovaná a kedy je najbližšie potrebné ju preskúmať. Ak politika ešte neexistuje, zaznamenajte to ako prioritné opatrenie.

Dostupné šablóny

Šablóny pre niekoľko nižšie uvedených politík sú zahrnuté v prílohách k týmto politikám:

- Zásady prijateľného používania: Dodatok III.
- Postup reakcie na incident: Dodatok IV.
- Posúdenie vplyvu na ochranu údajov (DPIA): Dodatok V.
- Register rizík: Dodatok VI.
- Register mapovania údajov: Dodatok VII.
- Sebahodnotenie kybernetickej odolnosti školy: Dodatok IX

Identifikácia	Názov politiky	Kľúčové oblasti pôsobnosti	Vlastník zásad	Posledná aktualizácia	Ďalšia recenzia
1	Zásady prijateľného používania (AUP)	Používanie školských systémov a zariadení. Pravidlá pre mobilné telefóny. Hlásenie.	Riaditeľ / IT koordinátor		
2	Politika riadenia prístupu	Kto má prístup k ktorým systémom a údajom. Pravidlá pre heslá. Odstránenie prístupu, keď zamestnanec odíde.	IT koordinátor / DPO		

Identifikácia	Názov politiky	Kľúčové oblasti pôsobnosti	Vlastník zásad	Posledná aktualizácia	Ďalšia recenzia
3	Zásady ochrany údajov	Súlad s GDPR. Zodpovednosti zodpovednej osoby za ochranu údajov. Súhlas rodičov. Oznámenia o ochrane osobných údajov. Reakcia na porušenie ochrany údajov.	Zodpovedná osoba za ochranu údajov / Riaditeľ		
4	Zásady zálohovania	Čo sa zálohuje, ako často, kde sa to ukladá a ako sa testuje obnova.	IT koordinátor		
5	Politika reakcie na incidenty	Ako škola reaguje na kybernetické incidenty a úniky údajov. Kto je zodpovedný. Ako informovať úrady.	Riaditeľ / ZO / IT koordinátor		
6	Zásady proti šikanovaniu (vrátane kyberšikanovania)	Definícia kyberšikany. Postup nahlasovania. Ako škola reaguje. Školenie zamestnancov. Zapojenie rodičov.	Riaditeľ		
7	Pravidlá pre mobilné zariadenia	Pravidlá pre študentské mobilné telefóny v súlade s vnútroštátnymi právnymi predpismi. Zákaz	Riaditeľ		

Identifikácia	Názov politiky	Kľúčové oblasti pôsobnosti	Vlastník zásad	Posledná aktualizácia	Ďalšia recenzia
		neoprávneného nahrávania.			

Dodatok IX: Sebahodnotenie kybernetickej odolnosti školy

Školy môžu tento kontrolný zoznam použiť na vytvorenie základného pochopenia svojej súčasnej kybernetickej odolnosti a na identifikáciu nedostatkov v prioritách. Každú položku označte ako Áno, Čiastočne alebo Nie. Účelom nie je dosiahnuť úspech alebo neúspech, ale identifikovať, na čo zamerať úsilie.

Školy sa vyzývajú, aby toto sebahodnotenie opakovali aspoň raz ročne. Sledovanie skóre v priebehu času pomáha monitorovať pokrok a podporuje kultúru neustáleho zlepšovania.

Uvedené položky sú orientačné. Prispôsobte ich tak, aby odrážali kontext vašej školy, národné požiadavky a špecifické okolnosti.

Doména	Čo skontrolovať	Áno / Čiastočne / Nie
Riadenie	Škola má určeného koordinátora kybernetickej bezpečnosti alebo digitálnej bezpečnosti.	
Riadenie	Škola má písomné Zásady prijateľného používania, ktoré boli revidované v priebehu posledných 2 rokov.	
Riadenie	Škola má zdokumentovaný postup reakcie na incidenty, s ktorým sú zamestnanci oboznámení.	
Povedomie a školenie	Zamestnanci absolvujú minimálne ročne školenie v oblasti kybernetickej bezpečnosti a online bezpečnosti.	

Doména	Čo skontrolovať	Áno / Čiastočne / Nie
Povedomie a školenie	Študenti dostávajú veku primerané vzdelávanie v oblasti digitálneho občianstva a online bezpečnosti.	
Povedomie a školenie	Rodičia a opatrovníci dostávajú informácie o digitálnych rizikách aspoň raz za školský rok.	
Blahobyt a prevencia	Škola má špecifický, pomenovaný protokol pre reakciu na kyberšikanu.	
Blahobyt a prevencia	Študenti vedia, ako a komu majú dôverne nahlásiť online incidenty.	
Blahobyt a prevencia	Preventívne aktivity sa výslovne zameriavajú na rozmanité a zraniteľné skupiny.	
Údaje a súkromie	Škola vedie register platforiem a nástrojov, ktoré spracovávajú údaje študentov.	
Údaje a súkromie	Súhlas rodičov sa získava pred zápisom študentov na digitálne platformy, ak to vyžaduje zákon.	
Technické opatrenia	Školské zariadenia a siete používajú aktuálny ochranný softvér a kontroly prístupu.	
Technické opatrenia	Pravidelne sa vytvárajú a testujú zálohy kritických školských údajov.	

Ako interpretovať svoje skóre

Počítajte odpovede Áno (1 bod) a odpovede Čiastočne (0,5 bodu). Vydeľte 13 a vynásobte 100, aby ste získali percento. Priraďte k úrovniam zrelosti uvedeným nižšie.

Úroveň	Skóre	Popis
1 - Iniciála	0 až 20 %	Malé alebo žiadne formálne postupy riadenia, školení alebo incidentov.
2 - Rozvíjanie	21 až 45 %	Základné zásady existujú, ale nie sú dôsledne uplatňované, prehodnocované ani komunikované.
3 – Založené	46 až 70 %	Základné prvky riadenia, školenia a reakcie na incidenty sú zavedené a zamestnanci sú im známe.

4 – Pokročilý	71 až 90 %	Komplexné, pravidelne revidované zásady a školenia oslovujú zamestnancov, študentov aj rodičov.
5 - Odolný	91 až 100 %	Kybernetická odolnosť je zakotvená v školskej kultúre prostredníctvom neustáleho vzdelávania a inkluzívnej prevencie.

Tieto úrovne slúžia len ako nástroj sebahodnotenia a nepredstavujú formálnu certifikáciu ani posúdenie zhody.

Referencie

Legislatíva Európskej únie

Nasledujúce právne nástroje Európskej únie tvoria spoločný právny rámec, na ktorom je založená táto politika. Stanovujú základné požiadavky na ochranu údajov, kybernetickú bezpečnosť, umelú inteligenciu, digitálne služby, elektronické komunikácie a digitálne vzdelávanie vo všetkých členských štátoch EÚ.

- Európska únia, Nariadenie (EÚ) 2016/679 (Všeobecné nariadenie o ochrane údajov – GDPR), Úradný vestník Európskej únie. Dostupné na: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
- Európska únia, smernica (EÚ) 2022/2555 (smernica NIS 2), Úradný vestník Európskej únie. Dostupné na: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555
- Európska únia, nariadenie (EÚ) 2024/1689 (zákon o umelej inteligencii), Úradný vestník Európskej únie. Dostupné na: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689
- Európska únia, nariadenie (EÚ) 2022/2065 (zákon o digitálnych službách), Úradný vestník Európskej únie. Dostupné na: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065
- Európska únia, smernica 2002/58/ES (smernica o súkromí v elektronických komunikáciách), Úradný vestník Európskych spoločenstiev. Dostupné na: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058
- Európska únia, nariadenie (EÚ) 2019/881 (zákon o kybernetickej bezpečnosti), Úradný vestník Európskej únie. Dostupné na: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881

Národné legislatívne nástroje

Pri príprave 2. časti tejto politiky boli použité nasledujúce národné legislatívne nástroje a oficiálne zdroje. Sú uvedené podľa krajín v súlade so štandardnou praxou odkazovania pre projekty financované z európskych zdrojov.

Grécko

- Grécka republika (2018). Zákon 4577/2018 o bezpečnosti sietí a informačných systémov. Vládny vestník A' 199/03.12.2018. Dostupné na: https://www.mindigital.gr/wp-content/uploads/2019/09/N.4577_2018.pdf
- Grécka republika (2019). Zákon 4624/2019 o ochrane fyzických osôb pri spracovaní osobných údajov (implementácia GDPR). Vládny vestník A' 137/29.08.2019. Dostupné na: https://www.dpa.gr/sites/default/files/2020-08/LAW%204624_2019_EN_TRANSLATED%20BY%20THE%20HDPA.PDF
- Grécka republika (2020). Zákon 4727/2020 o digitálnej správe vecí verejných a elektronických komunikáciách. Vládny vestník A' 184/23.09.2020. Dostupné na: https://adae.gov.gr/images/nomothetiko-plaisio/Nomos_4727_2020_01.pdf
- Grécka republika (2022). Zákon 4961/2022 o vznikajúcich technológiách a digitálnej správe vecí verejných. Vládny vestník A' 146/27.07.2022. Dostupné na: https://www.mindigital.gr/wp-content/uploads/2024/02/N-4961.pdf
- Grécka republika (2023). Zákon 5029/2023 o prevencii a riešení násilia a kyberšikany v školách. Vládny vestník A' 55/10.03.2023. Dostupné na: https://www.iep.edu.gr/wp-content/uploads/2025/01/2024-08-02_N_5029-2023.pdf

- Grécka republika (2024). Zákon 5160/2024 o kybernetickej bezpečnosti (transpozícia NIS2). Vládny vestník A' 195/27.11.2024. Dostupné na: https://search.et.gr/el/fek/?fekId=774154
- Ministerstvo digitálnej správy vecí verejných, Helénska republika (2025). Ministerské rozhodnutie 1689/2025 o požiadavkách na kybernetickú bezpečnosť pre subjekty verejného sektora. Vládny vestník B' 2186/06.05.2025. Dostupné na: https://cyber.gov.gr/wp-content/uploads/2025/05/20250202186.pdf
- Ministerstvo digitálnej správy vecí verejných, Helénska republika (2025). Ministerské rozhodnutie 1899/2025 o správe informačnej bezpečnosti pre verejné subjekty. Vládny vestník B' 4250/05.08.2025. Dostupné na: https://cyber.gov.gr/wp-content/uploads/2025/03/KYA_APOFASI_10-Feb-2025_FEK-463_DEFTERO-TEFHOS.pdf

Taliansko

- Talianska republika (2003). Legislatívny dekrét č. 196/2003 – Zákon o ochrane osobných údajov, zmenený a doplnený legislatívnym dekrétom č. 101/2018. Dostupné na: https://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali.pdf
- Talianska republika (2021). Zákon č. 109/2021, ktorým sa mení dekrét-zákon č. 82/2021 – Zriadenie Národnej agentúry pre kybernetickú bezpečnosť (ACN). Gazzetta Ufficiale, 4. 8. 2021. Dostupné na: https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.codiceRedazionale=21A04841
- Talianska republika (2024). Legislatívny dekrét č. 138/2024 – Transpozícia NIS2. Gazzetta Ufficiale, 01.10.2024. Dostupné na: https://www.gazzettaufficiale.it/eli/id/2024/10/01/24G00155/SG
- Ministerstvo školstva, Talianska republika (2020). Ministerský dekrét č. 89/2020 – Usmernenia pre digitálne integrované vyučovanie (DDI). Dostupné na: https://www.mim.gov.it/documents/20182/0/Decreto.pdf
- Ministerstvo školstva, Talianska republika (2024). Oznámenie MIM č. 5274/2024 – Obmedzenia používania smartfónov v školách. Dostupné na: https://www.mim.gov.it/-/nota-n-5274-dell-11-luglio-2024
- Ministerstvo školstva, Talianska republika (2025). Obežník MIM č. 3392/2025 – Obmedzenia používania mobilných telefónov v školách. Dostupné na: https://www.mim.gov.it/-/circolare-n-3392-del-16-giugno-2025
- Ministerstvo školstva, Talianska republika (2025). Ministerský dekrét č. 166/2025 – Usmernenia pre zodpovedné používanie umelej inteligencie v školách. Dostupné na: https://www.mim.gov.it/-/decreto-ministeriale-n-166-del-9-agosto-2025

Portugalsko

- Portugalská republika (2018). Zákon č. 46/2018 — Právny rámec pre bezpečnosť kybernetického priestoru (RFSC). Diário da República, 13.08.2018. Dostupné na: https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384
- Portugalská republika (2019). Zákon č. 58/2019 — Portugalský zákon o ochrane údajov (implementácia GDPR). Diário da República, 08.08.2019. Dostupné na: https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982
- Rada ministrov, Portugalská republika (2020). Rezolúcia č. 30/2020 — Akčný plán digitálnej transformácie (PATD). Diário da República, 2020. Dostupné na: https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/30-2020-132133788
- Portugalská republika (2025). Zákon č. 95/2025 – Zákaz používania smartfónov v školách (1. – 6. ročník). Diário da República, 03.07.2025.

- Portugalská republika (2025). Zákon č. 125/2025 — Transpozícia NIS2 (v účinnosti 3. apríla 2026). Diário da República, 04.12.2025. Dostupné na: Decreto-Lei n.º 125/2025, de 4 dezembro | DR
- Generálne riaditeľstvo pre vzdelávanie (DGE), Portugalsko. PADDE – Rámec akčného plánu digitálneho rozvoja škôl. Dostupné na: https://www.dge.mec.pt
- Centro Nacional de Cibersegurança (CNCS) / DGE, Portugalsko. SeguraNet – zdroje digitálnej bezpečnosti a kybernetickej bezpečnosti pre školy. Dostupné na: https://www.seguranet.pt
- Centro Nacional de Cibersegurança (CNCS), Portugalsko. CERT.PT — Národný tím reakcie na počítačové núdzové situácie. Dostupné na: https://www.cncs.gov.pt/pt/certpt/

Rumunsko

- Rumunská republika (2018). Zákon č. 190/2018 – Ochrana osobných údajov (implementácia GDPR). Úradný vestník Rumunska č. 651/26.07.2018. Dostupné na: https://portal.just.ro/101/Documents/LEGE__190_2018_date_cu_caracter_personal.pdf
- Rumunská republika (2023). Zákon č. 58/2023 o povinnostiach prevádzkovateľov sietí a informačných systémov v oblasti kybernetickej bezpečnosti. Úradný vestník Rumunska č. 214/15.03.2023. Dostupné na: https://legislatie.just.ro/Public/DetaliiDocument/265677
- Rumunská republika (2023). Zákon č. 198/2023 – Zákon o preduniverzitnom vzdelávaní. Úradný vestník Rumunska č. 613/05.07.2023. Dostupné na: https://edu.ro/sites/default/files/_fisiere/Minister/2023/Legi_educatie_Romania_educata/legi_monitor/Legea_invatamantului_preuniversitar_nr_198.pdf
- Vláda Rumunska (2024). Mimoriadne nariadenie (OUG) č. 155/2024 – Transpozícia NIS2 (schválené zákonom č. 124/2025). Úradný vestník Rumunska č. 1332/31.12.2024. Dostupné na: https://legislatie.just.ro/Public/DetaliiDocumentAfis/293121
- Ministerstvo školstva, Rumunsko (2024). Nariadenie č. 5707/2024 – Študentský štatút. Úradný vestník Rumunska č. 795/12.08.2024. Dostupné na: https://www.edu.ro/sites/default/files/_fisiere/Legislatie/2024/OM_5707_2024_Statut_elev.pdf
- Ministerstvo školstva, Rumunsko (2025). OMEC 6055-6058 – ROFUIP 2025 – 2026: Rámcové nariadenie pre organizáciu a fungovanie preduniverzitných vzdelávacích jednotiek. Úradný vestník Rumunska č. 819/04.09.2025. Dostupné na: https://www.edu.ro/ROFUIP

Slovensko

- Slovenská republika (2003). Zákon č. 596/2003 Z. o štátnej správe v školstve a školskej samospráve (zákon o školách a školských zariadeniach) v znení neskorších predpisov. Dostupné na: https://www.slov-lex.sk
- Slovenská republika (2008). Zákon č. 245/2008 Z. o výchove a vzdelávaní (školský zákon) v znení zákona č. 323/2025 Z. s účinnosťou od 1. januára 2025 (obmedzenia mobilných telefónov). Dostupné na: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2008/245/
- Slovenská republika (2018). Zákon č. 18/2018 Z. o ochrane osobných údajov (implementácia GDPR). Dostupné na: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2018/18/
- Slovenská republika (2018). Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti. Dostupné na: https://www.zakonypreludi.sk/zz/2018-69
- Slovenská republika (2024). Zákon č. 366/2024 Z. z. o kybernetickej bezpečnosti (transpozícia NIS2), účinný od 1. januára 2025. Dostupné na: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2024/366/20250101.html
- Ministerstvo školstva Slovenskej republiky (2025). Usmernenie č. 1/2025 k prevencii a riešeniu kyberšikany v školách a školských zariadeniach. Dostupné na: https://www.minedu.sk/data/att/d76/32441.fb1a83.pdf

- Ministerstvo školstva Slovenskej republiky (2025). Plán zodpovedného využívania umelej inteligencie vo vzdelávaní na roky 2025 – 2027. Dostupné na: https://ai.iedu.sk/

Normy ISO

Nasledujúce medzinárodne uznávané štandardy slúžili ako podklad pre vývoj praktických odporúčaní a opatrení v oblasti riadenia uvedených v tejto politike.

- Medzinárodná organizácia pre normalizáciu (ISO), ISO/IEC 27001:2022, Bezpečnosť informácií, kybernetická bezpečnosť a ochrana súkromia – Systémy riadenia bezpečnosti informácií – Požiadavky. Dostupné na: https://www.iso.org/standard/27001
- Medzinárodná organizácia pre normalizáciu (ISO), ISO/IEC 27002:2022, Bezpečnosť informácií, kybernetická bezpečnosť a ochrana súkromia – Kontroly bezpečnosti informácií. Dostupné na: https://www.iso.org/standard/75652.html
- Medzinárodná organizácia pre normalizáciu (ISO), ISO/IEC 27701:2025, Bezpečnostné techniky – Rozšírenie noriem ISO/IEC 27001 a ISO/IEC 27002 pre správu súkromných informácií – Požiadavky a usmernenia. Dostupné na: https://www.iso.org/standard/27701
- Medzinárodná organizácia pre normalizáciu (ISO), ISO 22301:2019, Bezpečnosť a odolnosť – Systémy riadenia kontinuity podnikania – Požiadavky. Dostupné na: https://www.iso.org/standard/75106.html
- Medzinárodná organizácia pre normalizáciu (ISO), ISO 31000:2018, Riadenie rizík – Pokyny. Dostupné na: https://www.iso.org/standard/65694.html

Výskum a dôkazy

Pri príprave 4. časti tejto politiky boli použité nasledujúce výskumné zdroje a publikácie.

- Európska komisia (2025). Detské hlasy o kyberšikane: Konzultácia s deťmi vo veku 12 – 17 rokov. Dostupné na: https://eu-for-children.europa.eu/cyberbullying_en
- Európska komisia (2025). Usmernenia k opatreniam na zabezpečenie vysokej úrovne súkromia, bezpečnosti a ochrany maloletých online. Dostupné na: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:C_202505519
- Európska komisia / Lepší internet pre deti (BIK+) / Sieť Insafe (2025 – 2026). Monitorovanie politík BIK a štatistiky liniek pomoci. Dostupné na: https://better-internet-for-kids.europa.eu/en
- Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA) (2022). Iniciatívy v oblasti vzdelávania v oblasti kybernetickej bezpečnosti v členských štátoch EÚ. Dostupné na: https://www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-the-eu-member-states
- OECD (2025). Aký je život detí v digitálnom veku? Dostupné na: https://www.oecd.org/en/publications/how-s-life-for-children-in-the-digital-age_0854b900-en.html
- Polanin, JR, Espelage, DL, Grotpeter, JK a kol. (2021). Systematický prehľad a metaanalýza intervencií na zníženie páchania kyberšikany a jej viktimizácie. Prevention Science. Dostupné na: https://link.springer.com/article/10.1007/s11121-021-01259-y
- Torgal, C. a Aksoy, C. (2022). Metaanalýza vplyvu školských programov prevencie kyberšikany na správanie kybernetických prihliadajúcich. School Psychology Review, 52(2). Dostupné na: https://www.tandfonline.com/doi/full/10.1080/2372966X.2021.1913037
- Regionálna kancelária Svetovej zdravotníckej organizácie pre Európu (2024). Zdravotné správanie detí školského veku (HBSC): Zistenia o šikanovaní a kyberšikane. Dostupné na: https://www.who.int/europe/initiatives/health-behaviour-in-school-aged-children-(hbsc)-study
- Kyberšikana a LGBTQ mládež: Systematický prehľad literatúry a odporúčania pre prevenciu a intervenciu (2018). Dostupné na: https://pmc.ncbi.nlm.nih.gov/articles/PMC7163911/

- Korelácie medzi závislosťou od sociálnych médií a úzkosťou, depresiou, stratou vedomia, osamelosťou a sebavedomím u študentov: Systematický prehľad a metaanalýza (2025). PLOS ONE. Dostupné na: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0329466