

ŠKOLNÍ PROGRAM PROTI KYBERŠIKANĚ

INTEGROVANÁ STŘEDNÍ ŠKOLA TECHNICKÁ, BENEŠOV

Školní rok 2026/2027

Platnost od: 1.9.2026

Schválil/a: Mgr. Jana Fialová, ředitelka školy

1. Účel, působnost a úvod

Škola považuje bezpečné a respektující prostředí za základní podmínku vzdělávání. Tento dokument stanovuje systém prevence, včasného rozpoznávání a řešení kyberšikany na ISŠT Benešov. Je určen žákům a zaměstnancům školy a je součástí systému primární prevence rizikového chování. Navazuje na Školní program proti šikanování, Preventivní program školy, školní řád a krizové postupy.

Dokument je přizpůsoben prostředí střední školy. Výroční zpráva ISŠT Benešov za školní rok 2024/2025 uvádí kyberšikanu mezi jevy, které řešil koordinátor primární prevence.

2. Vymezení kyberšikany

Kyberšikana je úmyslné ubližování, ponižování, zastrašování, vydírání nebo obtěžování prostřednictvím digitálních technologií a online prostředí. Může probíhat na sociálních sítích, v chatovacích a komunikačních aplikacích, třídních skupinách, e-mailu, online hrách, herních platformách, webových stránkách nebo dalších platformách.

3. Specifika kyberšikany

Kyberšikana se od klasické šikany liší zejména rychlostí šíření obsahu, možností širokého publika, obtížnou kontrolou dalšího sdílení, možností anonymity a tím, že útok může pokračovat i mimo školu. Dopad však může přímo zasahovat do bezpečí, vztahů a vzdělávání žáka.

4. Cíle programu

Cílem programu je předcházet vzniku kyberšikany, vytvářet bezpečné digitální prostředí, podporovat bezpečné chování v online prostředí, rozvíjet digitální a mediální gramotnost, posilovat odpovědnost žáků, učit bezpečně reagovat na online útoky, podporovat schopnost požádat o pomoc, zvyšovat kompetence zaměstnanců, včas rozpoznat varovné signály, zajistit jednotný postup školy a poskytovat podporu oběti.

5. Základní principy školy

Škola netoleruje ponižování, výhrůžky, vydírání, zneužívání osobních údajů ani šíření ponižujícího obsahu. Každý podnět je nutné brát vážně a posuzovat s ohledem na bezpečí žáka. Oběť není viníkem situace a nemá být vystavována veřejné konfrontaci ani nucena k veřejnému vysvětlování či konfrontaci s původcem.

6. Formy kyberšikany

Může jít zejména o urážky, zesměšňování, ponižování, výhrůžky, šíření pomluv, zveřejňování ponižujících fotografií nebo videí, vytváření falešných profilů, vydávání se za jinou osobu, vylučování ze skupin, zveřejnění soukromé komunikace, obtěžování, online vydírání nebo záměrné vyvolávání konfliktů.

7. Související digitální rizika

Prevence zahrnuje také sexting, sdílení intimního obsahu bez souhlasu, zveřejňování osobních údajů, zneužití identity, phishing, podvodné jednání, nebezpečné online výzvy a nenávistné projevy.

8. Falešné profily a zneužití identity

Vytváření účtů jménem jiné osoby, zneužití její fotografie nebo zveřejňování nepravdivého obsahu může poškodit pověst a bezpečí žáka. Doporučuje se uchovat důkazy a případ oznámit škole a podle závažnosti také příslušné platformě nebo Policii ČR.

9. Zveřejňování fotografií a videí

Fotografie nebo video pořízené ve škole či mimo ni nesmí být používány k ponižování, zesměšňování nebo vydírání. Škola vede žáky k respektování soukromí druhých a k odpovědnému nakládání s digitálním obsahem.

10. Sociální síť a třídní skupiny

Třídní chat ani uzavřená skupina nejsou automaticky bezpečným prostorem. Platí zásady slušné komunikace, zákaz ponižování a šíření citlivého obsahu. Členové skupiny nemají podporovat útok lajky, komentáři ani dalším sdílením.

11. Sexting

Sexting představuje vytváření nebo sdílení intimního digitálního obsahu. Rizikem je jeho další šíření, zneužití, nátlak nebo vydírání. Škola postupuje citlivě a bez obviňování osoby, jejíž obsah byl zneužit.

12. Sextortion a online vydírání

Při vydírání intimním nebo jiným citlivým obsahem žák nemá platit, posílat další materiály ani řešit situaci sám. Je nutné uchovat důkazy a bezodkladně informovat důvěryhodného dospělého. Při závažném ohrožení škola zvažuje zapojení Policie ČR.

13. Kybergrooming a nebezpečné kontakty

Manipulativní navazování kontaktu s cílem získat důvěru a následně žáka ohrozit je závažným rizikem. Žáci jsou vedeni k opatrnosti při komunikaci s neznámými osobami a k oznámení podezřelého jednání.

14. Kyberstalking

Opakované sledování, obtěžování, vyhrožování nebo snaha kontrolovat online aktivity může představovat závažné riziko. Při posuzování se zohledňuje intenzita, trvání a dopad na bezpečí žáka.

15. Doxxing a zveřejnění osobních údajů

Zveřejnění adresy, telefonu, fotografií nebo jiných údajů bez souhlasu může zvýšit riziko dalšího obtěžování nebo fyzického ohrožení. Takový případ je nutné řešit bez zbytečného odkladu.

16. Nenávistné projevy a diskriminace

Ponižování nebo útoky založené na osobních charakteristikách žáka jsou nepřípustné. Škola podporuje respekt k odlišnostem a postupuje podle závažnosti situace, školního řádu a platných předpisů.

17. AI, deepfake a manipulovaný obsah

Generativní umělá inteligence umožňuje vytvářet falešné fotografie, videa nebo zvuk. Takový obsah může být zneužit k ponižování nebo vydírání. Škola vede žáky k ověřování obsahu, odpovědnému používání AI a okamžitému oznámení zneužití.

18. Digitální stopa

Žáci jsou vedeni k vědomí, že zveřejněný obsah může být kopírován a šířen dále. Součástí prevence je odpovědné zveřejňování, ochrana vlastní pověsti a respektování soukromí druhých.

19. Bezpečnost účtů a bezpečné používání sítí

Žáci mají používat silná a jedinečná hesla, vícefaktorové ověřování, aktualizovaná zařízení a vhodné nastavení soukromí. Mají být opatrní při přijímání kontaktů a při zveřejňování fotografií, videí a osobních údajů. Hesla ani přístupové kódy se nesdílejí s ostatními.

20. Varovné signály

Mezi možné varovné signály patří náhlé změny nálady po používání telefonu, strach z otevření zpráv, vyhýbání se škole nebo spolužákům, stažení ze skupin, výrazná změna nebo pokles výkonu, opakované konflikty, úzkost, poruchy spánku, obavy či strach z konkrétní osoby nebo zveřejnění ponižujícího obsahu. Samotný signál kyberšikanu nepotvrzuje; situaci je třeba citlivě prověřit.

21. Prevence

Prevence probíhá ve výuce, třídnických hodinách, preventivních programech, besedách, workshopech a v rámci práce školního poradenského pracoviště. Škola podle možností využívá aktuální metodické a vzdělávací materiály. ISŠT ve své dokumentaci uvádí preventivní práci s žáky, aktualizaci preventivních dokumentů a řešení kyberšikany v rámci primární prevence.

22. Co má udělat žák, který je terčem útoku

Žák by měl podle možností nereagovat impulzivně, nevyhrožovat zpět, neplatit vyděrači, neposílat další materiály, uchovat důkazy, zablokovat útočníka, nahlásit obsah platformě a co nejdříve informovat dospělou osobu. Ve škole se lze obrátit na třídního učitele, školního metodika prevence, výchovného poradce, vedení školy nebo jiného důvěryhodného zaměstnance.

23. Co má udělat svědek

Svědek nemá útok podporovat, sdílet ani komentovat. Má-li informace o incidentu, měl by je oznámit dospělému a podle možností uchovat relevantní důkazy. Přihlízející může významně ovlivnit, zda se útok bude dále šířit.

24. Co má udělat pedagog

Pedagog zachová klid, zajistí bezpečí žáka, neobviňuje oběť, neřeší případ veřejnou konfrontací, předá informace školnímu metodikovi prevence nebo vedení školy a postupuje podle tohoto dokumentu a krizových postupů.

25. První reakce školy

1. Zajistit bezpečí žáka. 2. Zastavit další šíření, pokud je to možné. 3. Informovat školního metodika prevence nebo vedení. 4. Citlivě zjistit základní okolnosti. 5. Uchovat relevantní elektronické důkazy. 6. Posoudit závažnost případu. 7. Podle situace informovat zákonné zástupce. 8. Stanovit opatření na ochranu oběti a zastavení jednání. 9. Podle potřeby zapojit odborné instituce. 10. Provést následnou kontrolu.

26. Uchování elektronických důkazů

Důležité mohou být screenshoty, odkazy, uživatelská jména, časové údaje, e-maily, zprávy, fotografie nebo videa. Důkazy se nemají zbytečně upravovat ani rozesílat či dále šířit. Škola s nimi nakládá s ohledem na ochranu osobních údajů.

27. Práce s obětí

Škola poskytuje podporu, chrání žáka před dalším tlakem a podle potřeby zajistí poradenskou nebo odbornou pomoc. Podle situace může upravit dohled, zajistit poradenskou podporu a

doporučit odbornou pomoc. Oběť není nucena ke konfrontaci s původcem a její citlivé údaje se nezveřejňují.

28. Práce s původcem

Jednání se řeší podle závažnosti, školního řádu a platných předpisů. Podle situace může být využit pohovor, výchovné opatření, spolupráce s rodiči, odborná intervence a další opatření. Cílem je zastavení jednání, převzetí odpovědnosti a prevence opakování.

29. Práce s třídním kolektivem

Je-li incident spojen s třídou nebo skupinou, škola pracuje i s kolektivem. Zaměřuje se na bezpečí, odpovědnost přihlížejících, respekt a obnovení důvěry. Podle potřeby je přizván odborník.

30. Kyberšikana namířená proti zaměstnanci

Škola chrání také své zaměstnance. Závažné urážky, výhrůžky, falešné profily, ponižování nebo zveřejňování soukromého či ponižujícího obsahu proti zaměstnanci se řeší podle okolností, školního řádu a platných právních předpisů.

31. Spolupráce s rodiči

Rodiče jsou vedeni k otevřené komunikaci o online prostředí. Při podezření na kyberšikanu je vhodné kontaktovat školu co nejdříve. Rodiče mají pomoci uchovat důkazy a zabránit impulzivnímu jednání dítěte.

32. Spolupráce s odbornými institucemi

Podle závažnosti může škola spolupracovat s pedagogicko-psychologickou poradnou, PPP Benešov, střediskem výchovné péče, OSPOD, Policií ČR, zdravotnickými a psychologickými službami nebo dalšími odborníky. ISŠT Benešov již v rámci prevence spolupracuje s odbornými službami a Policií ČR.

33. Bezprostřední ohrožení

Při bezprostředním ohrožení života nebo zdraví škola nejprve zajistí bezpečí žáka a podle situace bezodkladně přivolá odpovídající pomoc. Následně informuje kompetentní pracovníky a postupuje podle krizových pravidel školy.

34. Evidence případů

O významných případech se vede dokumentace v rozsahu potřebném pro řádné řešení. Dokumentace je chráněna před neoprávněným přístupem a citlivý obsah se dále nešíří. Škola s dokumentací nakládá v souladu s pravidly ochrany osobních údajů.

35. Následná kontrola

Po vyřešení případu škola ověřuje, zda útok nepokračuje, nepřesunul se na jinou platformu nebo nedochází k odvetnému jednání. Podle potřeby pokračuje podpora oběti a práce s kolektivem.

36. Odpovědnost pracovníků školy

Ředitel/ka školy odpovídá za systém prevence a bezpečné prostředí. Školní metodik/metodička prevence koordinuje preventivní činnost. Výchovný poradce/poradkyně poskytuje poradenskou podporu. Třídní učitelé sledují klima třídy. Každý zaměstnanec školy věnuje pozornost bezpečí žáků a závažné podezření předává kompetentnímu pracovníkovi.

37. Kontakty

Aktuální kontakty pracovníků školy a odborných služeb jsou vedeny v interním adresáři školy. Veřejná verze dokumentu uvádí pouze obecné kontaktní údaje školy a vybrané veřejné služby v rozsahu určeném školou.

38. Vyhodnocování programu

Škola pravidelně vyhodnocuje výskyt kyberšikany, preventivní aktivity, podněty žáků a rodičů a účinnost přijatých opatření. Výsledky využívá při aktualizaci Preventivního programu školy a dalších preventivních dokumentů.

39. Závěrečná ustanovení

Tento dokument je součástí systému prevence ISŠT Benešov a je propojen se Školním programem proti šikanování, Preventivním programem školy, školním řádem a krizovými postupy. Aktualizuje se podle potřeb školy, vývoje digitálního prostředí a změn metodických či právních předpisů.

40. Použité zdroje

MŠMT – Metodické doporučení k primární prevenci rizikového chování č. j. 21291/2010-28 a příslušné tematické přílohy; MŠMT – metodické materiály k prevenci a řešení šikany; NÚKIB – vzdělávací materiály pro školy a střední školy zaměřené na kybernetickou bezpečnost; interní dokumenty a zkušenosti ISŠT Benešov. MŠMT uvádí metodické doporučení jako základní rámec pro primární prevenci a doporučené postupy škol.

Zpracovala: Mgr. Lucie Bílková, školní metodik prevence

26. 8. 2026

PŘÍLOHA Č. 1 – RYCHLÝ POSTUP PRO ŽÁKA

Někdo mě napadá online: 1. Neodpovídej v afektu. 2. Neplat' a neposílej další materiály. 3. Uchovej důkazy. 4. Zablokuj útočníka, pokud je to bezpečné. 5. Nahlas obsah platformě. 6. Řekni to dospělému.

PŘÍLOHA Č. 2 – RYCHLÝ POSTUP PRO PEDAGOGA

Zajistit bezpečí → neobviňovat oběť → informovat kompetentního pracovníka → uchovat důkazy → zjistit základní okolnosti → posoudit závažnost → informovat rodiče podle situace → stanovit opatření → zapojit odborníky podle potřeby → následně kontrolovat.

PŘÍLOHA Č. 3 – RYCHLÝ POSTUP PRO RODIČE

Zachovat klid → dítěti věřit → neobviňovat → nemažte důkazy → uložte screenshoty a odkazy → kontaktujte školu → při vydírání, výhrůžkách nebo akutním ohrožení vyhledejte odbornou či bezpečnostní pomoc.

PŘÍLOHA Č. 4 – KONTROLNÍ SEZNAM PŘI INCIDENTU

Bezpečí žáka zajištěno; informován kompetentní pracovník; zjištěny základní okolnosti; důkazy uchovány; posouzena závažnost; informování zákonní zástupci podle situace; stanovena opatření; zvážena odborná pomoc; pracováno s kolektivem; provedena následná kontrola; případ zaznamenán.

PŘÍLOHA Č. 5 – ZÁZNAM O INCIDENTU

Datum a čas oznámení: _____
Oznámil/a: _____
Třída: _____
Popis incidentu: _____
Použitá platforma: _____
Zapojené osoby: _____
Důkazy uchovány: ANO / NE
Přijatá opatření: _____
Informováni: _____
Odborná pomoc / instituce: _____
Následná kontrola dne: _____

ZÁVĚR

V Benešově dne [DATUM]

.....[JMÉNO A PŘÍJMENÍ]ředitel/ka školy