

## Příloha č. 7 - Kyberšikana

<p><b>Typ rizikového chování</b></p>	<p><b>Kyberšikanu</b> definujeme jako <b>zneužití ICT (informačních komunikačních technologií), zejména pak mobilních telefonů a internetu, k takovým činnostem, které mají někoho záměrně ohrozit, ublížit mu.</b> Podobně jako u šikany tváří v tvář se jedná o úmyslné chování, kdy je oběť napadána útočníkem nebo útočníky. Povaha a provedení útoku pak určuje její závažnost.</p> <p><b>Předpona kyber</b> - značí prostředí, ve kterém se šikana odehrává, tedy kybernetický svět počítačů, internetu a mobilních telefonů. Kyberšikana může samozřejmě probíhat i přes jiné technické komunikační prostředky, např. pagery, v české realitě jsou však v drtivé většině využívány právě výše zmíněné mobilní telefony a internet.</p>
<p><b>Atributy odlišnosti</b></p>	<p><b>Zvláštnosti kyberšikany oproti tradiční nepřímé (psychické) šikaně</b></p> <p>Oproti šikaně tváří v tvář má kyberšikana ze své podstaty mnohem větší dosah, čímž ještě více zhoršuje prožívání oběti. Pokud je oběť šikanována ve třídě, svědky pomluv, nadávek, posmívání a ztrapňování je max. několik desítek lidí. V prostředí internetu je svědkem (ale i útočníkem) stejného chování klidně i několik desítek tisíc lidí.</p> <p><b>Anonymita</b></p> <ul style="list-style-type: none"><li>• oběť o napadení leckdy ani nemusí dlouhou dobu vědět</li><li>• oběť není vždy schopná identifikovat či vystopovat agresora</li><li>• vnímání dopadu jednání (útočník nevidí přímou reakci oběti na útok)</li><li>• odosobněnost útoku</li></ul> <p><b>Čas</b></p> <ul style="list-style-type: none"><li>• útoky se prostřednictvím internetu šíří mnohem rychleji než v realitě</li><li>• probíhají bez přestávek - oběť je šikanována 24 hodin denně, 7 dní v týdnu.</li><li>• útok je možné provést kdykoli (0:00, při hodině matematiky, apod.)</li><li>• příprava a realizace útoku není časově limitována</li></ul> <p><b>Místo</b></p> <ul style="list-style-type: none"><li>• agresor může provést útok odkudkoli (škola, hřiště, kavárna, doma,....)</li><li>• není nutná přítomnost agresora a oběti na stejném místě</li></ul> <p><b>Proměna profilu agresora i oběti</b></p> <ul style="list-style-type: none"><li>• pro útok není nutná fyzická, psychická či sociální zdatnost (oběť „klasické šikany“ může být kyberagresorem)</li><li>• podmínkou provedení útoku je „kybergramotnost“ a její úroveň</li><li>• kyber - prostor je dostupný komukoli</li></ul>

## Řešení

- děti a mladí lidé za těmito projevy šikany vůbec nemusí vidět. A protože nepoznají, že se jedná o šikanu, neví, jak se s ní vypořádat.
- obtížnost zajištění rychlé ochrany oběti (odstranění profilu, SMS, ICQ....)
- často chybí svědci
- obtížně stopovatelný útočník
- nejednoznačný přístup k legislativě

## **Závislost související s využíváním ICT technologií**

Často se obětí kyberšikany stávají děti, které jsou **na internetu nebo mobilním telefonu závislé. Sociální kontakty navazují především** ve virtuálním světě, ve skutečném světě nemají příliš kamarádů.

Čím více jsou ICT technologie využívány a jejich potřeba se stává nedílnou součástí běžného života, tím se zároveň zvyšuje riziko napadení. Pro školní prostředí to znamená - v případě využívání ICT technologie (intranet, www, profil,...), nutnost vyššího zabezpečení.

### **Typy kyberšikany:**

**1. Přímá kyberšikana:** útočník → oběť

**2. Kyberšikana v zastoupení:** útočník → třetí osoba → oběť

### **Nejčastější motivy kyberagresora** (řazeny od nejzávažnějšího po nejméně závažný typ)

- Snaží se ovládat druhé prostřednictvím strachu, touží po moci. Obvykle potřebují pro svou činnost publikum.
- Znuděný, hledá zábavu, narcistický... Kyberšikana je obvykle páchána ve skupině, nebo je ve skupině alespoň plánována.
- Bere právo do svých rukou (zlonpravující, uděluje lekci,...). Pracují většinou sami, ale mohou své aktivity a motivy sdílet se svými nejbližšími přáteli.
- Má tendenci odpovídat ve vzteku nebo frustraci – pomsta, kompenzace. (někdy může být obětí klasické šikany)
- Má sklon vystupovat na internetu jako někdo jiný. Zneužívat ICT technologie, bez vědomí závažnosti tohoto jednání. Motivem jsou dva hlavní důvody: a) Můžu b) Je to legrace.

### **Principy (proč to pachatelé dělají):**

- Uvolnění
- Uznání
- Posílení pocitu sounáležitosti
- Demonstrace síly
- Strach

	<p><b>Příčiny a spouštěče:</b></p> <ul style="list-style-type: none"> <li>• Je to „normální“</li> <li>• Nuda</li> <li>• Kulturní konflikty</li> <li>• Spory ve třídě</li> <li>• Rozpad přátelství</li> <li>• Proměna třídního kolektivu</li> <li>• Zveřejnění osobních informací</li> </ul> <p><b>Kdy se škola má začít zabývat kyberšikanou?</b> Škola by se kyberšikanou měla zabývat vždy, když se o ní dozví. Základním úkolem musí být zmapování konkrétního případu, které nám pomůže se rozhodnout pro správný postup řešení. Poslouží k tomu zodpovězení tří otázek: Týká se kyberšikana žáka mé školy? Jak jsem se informaci dozvěděl? Děje se kyberšikana během vyučování?</p> <p><b>Pro řešení kyberšikany potřebujeme počítačovou gramotnost</b></p> <ul style="list-style-type: none"> <li>• ICT technologie nejsou špatné, ale záleží jen na nás, zda je využijeme ve svůj prospěch či neprospěch</li> <li>• <b>nutná spolupráce ŠMP a TU s odborníkem IT</b> (zálohování dat, zajištění stop,...)</li> <li>• prověřit všechny možnosti napadení (SMS, youtube, profil, email, www....)</li> <li>• základní znalost a povědomí o využívání mobilů a ICT technologií</li> </ul>
<p><b><i>U každého podezření o výskytu daného jevu musí být vždy informován ředitel školy/šk. zařízení.</i></b></p>	
<p><b>Kdo řeší + s kým spolupracuje</b></p>	<p>školní metodik prevence s výchovným poradcem, školním psychologem, třídním učitelem, se školským poradenským zařízením, pediatrem</p>
<p><b>Na základě čeho</b> (legislativa, dokumenty apod.) se problém řeší</p>	<p><b>Musíme využívat propojenost kyberšikany s tradiční školní šikanou</b></p> <p>Kyberšikana bývá u dětí školního věku často doplňkem klasické přímé a nepřímé šikany. Je tedy důležité při řešení prověřit případné souvislosti s klasickou šikanou. Tedy pokud probíhá klasická šikana (př. nadávky, ponižování...), je nutné zjistit situaci oběti v kyberprostoru (mobil, profil, chat,...) a naopak.</p> <p>Oběť klasické šikany se může stát agresorem v kyberšikaně.</p> <p>Řešení kyberšikany vyžaduje kvalitní odhad situace (vyhodnocení, zda jde o kyberšikanu a zda je škola kompetentní ji řešit) a znalost zásad práce klasické šikany (dbát na posloupnost a načasování jednotlivých kroků řešení).</p> <p>V právní praxi bývá pojem šikana používán jako synonymum pro „úmyslné jednání, které</p>

je namířeno proti jinému subjektu, a které útočí na jeho důstojnost". Z hlediska výkladu pojmu šikanování není důležité, zda k němu dochází slovními útoky, fyzickou formou, nebo hrozbou násilí. Rozhodující je, kdy se tak děje úmyslně.

#### **Dále musí být splněny tyto podmínky**

- pachatel se dopustil jednání, které splňuje znaky konkrétního trestného činu tak, jak jsou vymezeny v trestním zákoně
- musí být prokázán úmysl pachatele dopustit se takového jednání a míra společenské nebezpečnosti
- jeho jednání dosahuje intenzity uvedené v zákoně

U trestných činů, jejichž podstatou byla šikana, lze proto předpokládat, že právě s ohledem na rozšiřující se případy podobných jednání bude skutek za trestný čin považován. Šikana bývá nejčastěji postihována podle ustanovení trestního zákona, a to jako:

- trestný čin omezování osobní svobody
- trestný čin vydírání
- trestný čin vzbuzení důvodné obavy
- trestný čin loupeže
- trestný čin ublížení na zdraví
- trestný čin poškozování cizí věci
- trestný čin znásilnění či pohlavního zneužívání

K tomu, aby byl pachatel postižen, musí být starší 15 let (15-18 let mladiství).

K trestní odpovědnosti mladších 15 let nedochází, neznamená to však, že nemohou být postiženi jinak, případně mohou být postiženi rodiče.

Nezletilý pachatel může být postižen nařízením ústavní výchovy, může nad ním být stanoven dohled.

Pokud jde o trestní sazby, je v případě šikany možný i jednočinný skutek, tzn. že jedno jednání může být kvalifikováno jako více trestných činů.

Pokud k šikanování došlo v průběhu vyučování, nese plnou odpovědnost škola. Prokáže-li se zanedbání ředitele školy nebo některého pedagoga, může být právně nebo pracovněprávně potrestán. Na školském zařízení lze v oprávněných případech požadovat i náhradu škody vzniklé v důsledku šikany. A to jak náhradu na věcech, tak na zdraví, včetně způsobené psychické újmy. Pokud dítě v důsledku šikany nemohlo např. docházet do školy (vyšší stupeň šikany), nese školské zařízení odpovědnost i škody vzniklé rodičům dítěte v důsledku např. uvolnění ze zaměstnání, zajištění hlídání dítěte, zajištění doprovodu do a ze školy apod.

	<p>Převzato z: KOLÁŘ, Michal, Bolest šikanování, Praha, Portál, 2001, s. 213 – 218. Upraveno podle: <a href="http://www.poradenskecentrum.cz">www.poradenskecentrum.cz</a></p> <p><b>Další možná legislativní východiska:</b></p> <ul style="list-style-type: none"> <li>• ublížení na cti <a href="http://www.portal.gov.cz">www.portal.gov.cz</a> – (v sekci &gt; zákony – zákon č. 200/1990 sb., zákon o přestupcích, § 49)</li> <li>• pomluva <a href="http://www.portal.gov.cz">www.portal.gov.cz</a> – (v sekci &gt; zákony – zákon č. 40/2009 sb., trestní zákoník, § 184)</li> <li>• zákaz natáčení, fotografování a zveřejnění snímků bez souhlasu dotyčné osoby <a href="http://www.portal.gov.cz">www.portal.gov.cz</a> – (v sekci &gt; zákony – zákon č. 40/1964 sb., občanský zákoník, § 12-13)</li> <li>• stalking <a href="http://www.portal.gov.cz">www.portal.gov.cz</a> – (v sekci &gt; zákony – zákon č. 40/2009 sb., trestní zákoník, § 353-354)</li> </ul>
<p><b>Jak postupovat z pozice školy</b></p>	<p><b>Co může dělat škola:</b></p> <ul style="list-style-type: none"> <li>• <b>Zaneste do školního řádu</b> pravidla používání ICT, intranetu a mobilních telefonů (během vyučování, přestávkách, v prostorách školy,...). Pravidla a jednotlivá doporučení najdete v příručce „Kybešikana a její prevence“ umístěné na <a href="http://www.kapezet.cz">www.kapezet.cz</a> – kyberšikana</li> <li>• <b>Informujte žáky</b> o netiketě a „listině práv na internetu“</li> <li>• <b>Instalujte a využívejte software</b>, který v učebnách vyučujícímu umožňuje informovat se přes svůj počítač, co právě žák na své ploše dělá nebo zaznamenává provoz. (informujte o tomto opatření žáky a systém nezneužívejte!)</li> <li>• <b>Bud'te vzorem</b> vhodného užívání moderních technologií</li> <li>• Pracujte na povědomí</li> <li>• Definujte kompetence v rámci školy</li> <li>• Definujte kompetence mimo školu</li> <li>• Začleňte téma do výuky</li> <li>• Vzdělávejte pedagogy</li> <li>• Podporujte pozitivní využívání technologií</li> </ul> <p><b>Co může dělat pedagog:</b></p> <ul style="list-style-type: none"> <li>• Posílit empatii mezi žáky</li> <li>• Pracovat na klimatu</li> <li>• Vést k úctě k druhým</li> <li>• Dávat pozitivní zpětnou vazbu</li> <li>• Vytvářet dobré vztahy</li> </ul>

<b>Z pozice oběti a rodiče</b>	<p><b>Co dělat?</b></p> <ol style="list-style-type: none"> <li><b>1. Zajistěte ochranu oběti</b> Kontaktujte operátora mobilní sítě nebo zřizovatele www stránek, profilu...atd.</li> <li><b>2. Zajistěte dostupné důkazy s podporou IT kolegy</b></li> <li><b>3. Důkladně vyšetřete a žádejte odbornou pomoc</b> Vyšetřete všechny souvislosti se zjištěným incidentem. Zajistěte si podporu a pomoc externího pracovníka (IT expert, PPP, policie,...). Kontaktujte a spolupracujte s MySpace, Facebookem, nebo jakýmkoli jiným webovým prostředím, kde ke kyberšikaně došlo.</li> <li><b>4. Opatření</b> Zvolte takové opatření a řešení, které je odpovídající závažnosti prohřešku a důsledkům, které agresor způsobil.</li> <li><b>5. Informujte a poučte rodiče</b> Informujte rodiče oběti i rodiče kyberagresora. Postup a zásady sdělování informací jsou stejné jako u „klasické šikany“ (např. NE konfrontace oběti a agresora). <b>Poučte rodiče</b> o tom, koho mohou (je vhodné) kontaktovat (Policie ČR, OSPOD, PPP, právní zástupce atd.). Některé případy kyberšikany nespadají do kompetence školy.</li> <li><b>6. Žádejte konečný verdikt a informace</b> Při zapojení a následně celém prošetření případu trvejte na konečném stanovisku všech zainteresovaných institucí (PČR...) a dalších subjektů (rodiče).</li> <li><b>7. Postihy</b> Při postizích agresorů postupujte v souladu se Školním řádem a již vypracovaným krizovým plánem.</li> </ol>
	<p><b>Oběti je třeba doporučit, aby:</b></p> <ul style="list-style-type: none"> <li>• Neodpovídala</li> <li>• Ukládala důkazy (screenshoty)</li> <li>• Mluvila o tom, co se jí děje</li> </ul> <ol style="list-style-type: none"> <li><b>1. Ukončete komunikaci</b> Nekomunikujte s útočníkem, nesnažte se ho žádným způsobem odradit od jeho počínání, nevyhrožujte, nemstěte se. Cílem útočníka je vyvolat v oběti reakci, ať už je jakákoli.</li> <li><b>2. Blokuje útočníka</b> Zamezte útočníkovi přístup k vašemu účtu nebo telefonnímu číslu a je-li to v dané situaci možné, i k nástroji či službě, pomocí které své útoky realizuje (kontaktujte poskytovatele služby).</li> <li><b>3. Oznamte útok, poradte se s někým blízkým, vyhledejte pomoc</b> Svěřte se blízké osobě. Pro uchování důkazů oslovte někoho, kdo má vyšší IT gramotnost. Kontaktujte školu a specializované instituce (PPP, policii, SVP, intervenční služby specializující se na řešení kyberšikany, psychology apod.).</li> <li><b>4. Uchovejte důkazy</b> Uchovejte a vystopujte veškeré důkazy kyberšikany (SMS zprávy, e-mailové zprávy, zprávy z chatu, uložte www stránky apod.). Na základě těchto důkazů může být proti útočníkovi či útočníkům zahájeno vyšetřování. (postup viz příloha).</li> <li><b>5. Žádejte konečný verdikt</b></li> </ol>

	<p>Po prošetření celého případu trvejte na konečném stanovisku všech zainteresovaných institucí.</p> <p><b>Pro rodiče</b></p> <ul style="list-style-type: none"> <li>• <b>Zajistěte, aby dítě vědělo</b>, že všechna pravidla chování při kontaktu s ostatními lidmi jsou stejná jako v reálném životě</li> <li>• <b>Ujistěte se</b>, že vaše škola má vhodný vzdělávací program o bezpečnosti na internetu.</li> <li>• <b>Učte své děti vhodnému chování</b> na internetu. Seznamte je s pravidly používání internetu či mobilního telefonu.</li> <li>• <b>Bud'te vzorem</b> vhodného užívání moderních technologií.</li> <li>• <b>Sledujte aktivity</b> svých dětí, když jsou online. Zajímejte se o to, k čemu vaše dítě mobilní telefon či internet používá.</li> <li>• <b>Používejte filtrační a blokační software</b></li> <li>• <b>Všímejte si varovných znaků</b> toho, že se děje něco neobvyklého. Jak se dítě při elektronické komunikaci chová, včetně reakcí dítěte na vaši přítomnost.</li> <li>• <b>Použijte „Smlouvu o používání internetu“</b> viz <a href="http://www.kapezet.cz">www.kapezet.cz</a> – Kyberšikana</li> <li>• <b>Kultivujte a udržujte</b> se svými dětmi otevřenou a upřímnou linii komunikace. Dejte dítěti najevo, že za vámi může přijít s problémem</li> </ul>
<p><b>V jakém případě vyrozumět Polici ČR/OSPOD</b></p>	<p>Pokud má učitel jistotu, že byl spáchán trestný čin, má ze zákona povinnost obrátit se na orgány činné v trestním řízení, pokud má podezření, zákon určuje školskému zařízení za povinnost nahlásit tuto skutečnost obecnímu úřadu, tedy sociálnímu pracovníkovi z orgánu sociálně právní ochrany dětí (OSPOD). V případě, že se rodiče odmítají spolupracovat se školou a odmítají se zúčastňovat výchovných komisí, je škola opět oprávněna vyrozumět OSPOD.</p>
<p><b>Co by mělo být cílem řešení</b></p>	<p>Učitelé, pedagogičtí pracovníci, vychovatelé, atd. by měli vědět, že v současné době žádné prostředí, kde se zdržuje více dětí delší dobu pohromadě, není vůči šikaně imunní. V těchto kolektivech je třeba zvýšeně věnovat pozornost různým příznakům skrytého násilí, jak fyzického tak psychického, které by šikanu mohly signalizovat, důsledně se věnovat prevenci, vytvořit kolektiv se zásadou, že silný chrání slabšího, kolektiv, kde vládne duch práva a spravedlnosti, důvěra k autoritě a vzájemná solidarita.</p>
<p><b>Doporučené odkazy</b></p>	<p>Nejlepší je ta pomoc, která je nejbližší a může být nejrychlejší. Zkuste se obrátit na pedagogicko-psychologickou poradnu, středisko výchovné péče, nebo jakéhokoli psychologa v místě bydliště. V případě, že máte pocit, že Vám nikdo nepomáhá, oslovte školské odbory orgánů místní samosprávy nebo českou školní inspekci.</p> <p><b><a href="http://www.saferinternet.cz">www.saferinternet.cz</a></b> (Informace na téma kyberšikana, ochrana osobních údajů aj. V sekci „Ke stažení“ výsledky výzkumu chování dětí na Internetu)</p> <p>.....</p> <p><b><a href="http://www.bezpecne-online.cz">www.bezpecne-online.cz</a></b> (Stránky pro teenagery, rodiče a učitele s informacemi o</p>

bezpečném používání internetu, prevenci a řešení kyberšikany; výukové materiály)

.....  
**www.protisikane.cz** (Informace o kyberšikaně a jejích projevech, tipy pro rodiče)

.....  
**www.minimalizacesikany.cz** (Praktické rady pro rodiče, učitele a děti, jak řešit šikanu a jak jí předcházet. V sekci „Pro média“ tisková zpráva s výsledky šetření o kyberšikaně na školách)

.....  
**http://prvok.upol.cz** (Centrum prevence rizikové virtuální komunikace UPOL, v sekci „Výzkum“ výsledky výzkumného šetření Kyberšikana u českých dětí)

.....  
**www.sikana.org** (Stránky občanského sdružení Společenství proti šikaně – aktuality z oblasti, související odkazy apod.)

**E-Bezpeci (www.e-bezpeci.cz)** - projekt zaměřený na prevenci rizikového chování na Internetu (kyberšikana, kybergrooming, kyberstalking, sociální sítě, sociální inženýrství, sexting atd.).

**Poradna E-Bezpeci (www.napisnam.cz)** - poradenská linka zaměřená na prevenci rizikového chování na Internetu, jen za letošní rok řešila přes 100 případů kyberšikany, stalkingu, sextingu apod.

projekt **E-Nebezpeci** pro učitele (**www.e-nebezpeci.cz**), který obsahuje řadu prezentací pro učitele

**www.hoax.cz**

**http://www.bezpecnykraj.cz/ebezpecnost**

[Kyberšikana a její prevence, příručka pro učitele](#)

<http://www.kapezet.cz/index.php?object=General&articleId=211&leveMenu=>

**Přehledový list Kyberšikana ke stažení (E-bezpečí) -**

[http://cms.ebezpeci.cz/component/option,com\\_docman/task,cat\\_view/gid,45/Itemid,2/lang,czech](http://cms.ebezpeci.cz/component/option,com_docman/task,cat_view/gid,45/Itemid,2/lang,czech)

**Leták Bezpečný Internet (E-bezpečí)**

[http://cms.ebezpeci.cz/component/option,com\\_docman/task,cat\\_view/gid,45/Itemid,2/lang,czech/](http://cms.ebezpeci.cz/component/option,com_docman/task,cat_view/gid,45/Itemid,2/lang,czech/)

**Příručka pro rodiče a vychovatele (Saferinternet)**

[http://www.saferinternet.cz/data/articles/down\\_696.pdf](http://www.saferinternet.cz/data/articles/down_696.pdf)

**Kontakty:**

[Poradna](#) webu Minimalizace šikany

**Domácí webové stránky s tematikou šikany:**

Společenství proti šikaně , [www.sikana.org](http://www.sikana.org)

Internet poradna, [www.internetporadna.cz](http://www.internetporadna.cz)



Sdružení Linka bezpečí (116 111) , [www.linkabezpeci.cz](http://www.linkabezpeci.cz)

Amnesty International ČR, [www.amnesty.cz](http://www.amnesty.cz)

### **Zahraníční webové stránky s tematikou šikany:**

Evropská observatoř pro násilí ve školách : [www.obsviolence.com/english/members/](http://www.obsviolence.com/english/members/)  
[www.bullying.co.uk](http://www.bullying.co.uk)

[www.bullying.org/public/frameset.cfm](http://www.bullying.org/public/frameset.cfm)

[www.schoolsecurity.org/trends/bullying.html](http://www.schoolsecurity.org/trends/bullying.html)

[www.nldontheweb.org/Banks\\_1.htm](http://www.nldontheweb.org/Banks_1.htm)

### **Příloha č.1**

#### **Legislativní rámec**

- **Školský zákon** (zákon 561/2004 Sb.)
- **Trestní zákoník** (zákon 40/2009 Sb.)
  - Trestné činy proti svobodě
    - § 175 Vydírání
    - § 176 Omezování svobody vyznání
  - Trestné činy proti právům na ochranu osobnosti, soukromí a listovního tajemství
    - § 182 Porušení tajemství dopravovaných zpráv
    - § 183 Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí
    - § 184 Pomluva
  - Trestné činy proti lidské důstojnosti v sexuální oblasti
    - § 191 Šíření pornografie
    - § 192 Výroba a jiné nakládání s dětskou pornografií
    - § 193 Zneužití dítěte k výrobě pornografie
  - Trestné činy proti rodině a dětem
    - § 202 Svádění k pohlavnímu styku
  - Trestné činy proti majetku
    - § 230 Neoprávněný přístup k počítačovému systému a nosiči informací
    - § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat
    - § 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti
  - Trestné činy obecně ohrožující
    - § 287 Šíření toxikomanie
  - Trestné činy narušující soužití lidí
    - § 352 Násilí proti skupině obyvatelů a proti jednotlivci
    - § 353 Nebezpečné vyhrožování
    - § 354 Nebezpečné pronásledování
    - § 355 Hanobení národa, rasy, etnické nebo jiné skupiny osob

- § 356 Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod
- **Občanský zákoník** (zákon 40/1964 Sb.)
  - § 11, 12, 13, 15, 16 Ochrana osobnosti
  - § 19b, odst. 2 a 3 o neoprávněném použití názvu právnické osoby
  - § 424 Odpovědnost za škodu způsobenou úmyslným jednáním proti dobrým mravům
- **Zákon o elektronických komunikacích** (127/2005 Sb.)
  - § 67 Identifikace zlomyslných nebo obtěžujících volání
  - § 93 Zneužití elektronické adresy odesílatele
- **Zákon o ochraně osobních údajů** (101/2000 Sb.)
  - § 10
  - § 44, odst. 2, písmeno c
  - § 44a, odst. 3

## Příloha č.2

### **Zbraně (praktiky) kyberšikan**

- Mobil
  - SMS/MMS/video nevhodného obsahu (urážení, zastrašování...)
  - volání, prozvánění
  - natáčení/focení a následné zveřejňování natočeného/vyfoceného (rozesílání dalším lidem, umístění na YouTube apod.)...
- Internet
  - Zakládání falešných profilů nebo změna původního
  - Zakládání profilů proti nějaké osobě
  - E-maily nevhodného obsahu
  - Krádež hesel a následné zneužití účtů
  - Obtěžování přes webkamery a IM (ICQ, Skype...)

### **Pojmy a možnosti související s užíváním IT technologií a kyberšikanou**

#### **Možnosti internetu**

Zdroj informací, možnost sdílení a sdělení informací (email, soubory, videa, články, blogy, web stránky, profily...), komunikace, hry, nákup a prodej zboží-slужeb, e-bankovníctví, sex...

#### **Možnosti mobilu**

Komunikační prostředek: volání, SMS, MMS zprávy, fotografování, video dokumentace, internet v mobilu (viz výše), MP3 (hudba), hry...

#### **Možnosti připojení**

Bezdrátová, pevná, mobilní komunikační technologie k propojení mezi dvěma a více elektronickými zařízeními, jakými jsou například mobilní telefon, PDA, osobní počítač nebo náhlavní souprava (kabel, bluetooth, Wi-Fi, infra, mobilní operátoři,.....)

#### **Internetové prohlížeče**

**Webový prohlížeč** (též **browser**) je počítačový program, který slouží k prohlížení **World Wide Webu (WWW)**. Program umožňuje komunikaci s HTTP serverem a zpracování přijatého kódu (HTML, XHTML... apod.), **který podle daných standardů** zformátuje a **zobrazí webovou stránku**. Textové prohlížeče zobrazují stránky jako text (obrázky apod.) obvykle velmi jednoduše formátovaný.

**Nejznámější jsou:** Windows **Internet Explorer**, [Mozilla Firefox](#), Safari, Google Chrome, Opera

### **Internetové vyhledávače**

**Internetový vyhledávač** je služba, která umožňuje na Internetu **najít webové stránky**, které obsahují požadované informace. Uživatel zadává do rozhraní vyhledávače klíčová slova, která charakterizují hledanou informaci a vyhledávač obratem na základě své databáze vypisuje seznam odkazů na stránky, které hledané informace obsahují.

**Nejznámější jsou:** **Google** – [www.google.cz](#) (com), **Seznam** – [www.seznam.cz](#), Atlas, Centrum, ICQ, Yahoo a další.

**Používané www profily :** [www.facebook.com](#) , [www.lide.cz](#), [www.myspace.com](#), [www.spoluzaci.cz](#) a další...

### **Komunikační programy**

**ICQ** (I seek you – hledám tě) - posílání textových zpráv, offline posílání zpráv, skupinové chatování odesílání SMS zpráv, odesílání souborů a hry.

**Skype** – telefonování, posílání textových zpráv, offline posílání zpráv, skupinové chatování odesílání SMS zpráv, odesílání souborů...  
a další...

**Video on – line - Youtube** – [www.youtube.com](#) - YouTube je největší internetový server pro sdílení video a audio souborů.

## **Příloha č.3**

### **Co není kyberšikana...**

Za kyberšikana nemůžeme označit veškeré zavrženíhodné chování v prostředí moderních technologií. Zmiňme několik příbuzných fenoménů, které jsou sice také nebezpečné, ale nejsou kyberšikanou.

**Kyberstalking** – pronásledování prostřednictvím moderních technologií. Zahrnuje opakované a intenzivní telefonování, psaní SMS, e-mailů, vzkazů na sociálních sítích apod. Na toto jednání pamatuje trestní zákoník (zákon 40/2009 Sb.) v § 354, odst. 1, písmeno c: Kdo jiného dlouhodobě pronásleduje tím, že jej vytrvale prostřednictvím prostředků elektronických komunikací, písemně nebo jinak kontaktuje a toto jednání je způsobilé vzbudit v něm důvodnou obavu o jeho život nebo zdraví nebo o život a zdraví osob jemu blízkých, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti.

**Kybergrooming** – nebezpečné chování dospělých osob, které se prostřednictvím manipulativních technik a navázáním „přátelství“ v internetovém prostoru snaží dostat své oběti na schůzku v reálném světě. Cílem jejich počínání bývá sexuální zneužití, točení a

focení pornografie, nucení k prostituci. Nejohroženější skupinou jsou děti a dospívající ve věku 6 – 15 let.

**Happy Slapping** – volně přeloženo jako „veselé fackování“. Jde o obětí nevyprovokovaný útok, kdy útočník využije momentu překvapení náhodně vybrané osoby (v parku, na ulici, v metru...), kterou následně zbijí. Komplic vše natáčí na mobilní telefon a video se rvačkou je poté umístěno na internet, např. na YouTube.

**Sexting** – distribuce fotografií a videomateriálů intimního charakteru bez souhlasu zobrazené osoby. Buď tyto materiály pořizují oběti samy, s úmyslem zaujmout nebo vyhovět svému partnerovi, nebo jsou pořizovány bez jejich vědomí. Útočník tyto materiály pak buď rozesílá všem svým známým pro „pobavení“, nebo se stanou prostředkem vydírání oběti.

**Další pojmy** najdete v metodickém materiálu o Kyberšikaně zde:

[http://www.kapezet.cz/admin/data/articleFiles/211/soubor\\_2809486.pdf](http://www.kapezet.cz/admin/data/articleFiles/211/soubor_2809486.pdf)

#### Příloha č.4

##### **Týká se kyberšikana žáka mé školy (ať už v pozici oběti či útočníka)?**

→ **Ne:** Jak jsem se informaci dozvěděl?

→ Nahlásil mi to můj žák: Pokud k vám mají děti důvěru, mohou se vám svěřovat i s problémy např. svých kamarádů z jiných škol. Měli byste žáka vyslechnout a dát mu praktické rady, kam se jeho kamarád může obrátit pro pomoc, jak má zajistit důkazy apod. Zeptejte se po pár dnech svého žáka, který vám věc nahlásil, jak vše pokračuje. Leckdy může znamenat „kamarádovi se stalo“ naopak „mně se děje, ale ještě nemám odvahu o tom mluvit“.

→ Zaslchl(a) jsem to z důvěryhodných zdrojů: Zde záleží na vašem přístupu, zda se v případě chcete osobně angažovat, např. radou. Není to věc školy.

→ **Ano:** Děje se kyberšikana během vyučování?

→ **Ne:** Škola nemůže udělovat kázeňské tresty, popř. snížené známky z chování za činnost, která se nestala během vyučování. To ovšem neznamená, že by škola neměla kyberšikana řešit alespoň v následujících základních bodech:

- Zjistěte informace o tom, jakých všech tříd se případ kyberšikany týká. Ve všech zasažených třídách pak proveďte sociometrii – z 80% je kyberšikana pouze doplňkem šikany tváří v tvář, a proto je velice pravděpodobné, že šikana ve vaší škole probíhá. Pokud se toto podezření potvrdí, postupujte podle zpracovaného krizového plánu na šikanu.
- Doporučte rodičům oběti, aby se v případě kyberšikany svého dítěte obrátili na Policii ČR, popř. podali žalobu k soudu.
- Informujte (se souhlasem zletilého žáka nebo zákonného zástupce žáka

nezletilého) zasažené žáky o postupu při řešení kyberšikany. Sdělte jim, že škola trestat v tomto případě nemůže, a proto byl případ předán policii/soudu. Děti potřebují vědět, že za každé nepřiměřené chování přijde trest.

→ **Ano:**

- Škola pomůže oběti zajistit důkazy.
- Škola postupuje podle krizového plánu na šikanu.
- V závažnějších případech kyberšikany (kyberšikana naplňuje skutkovou podstatu trestného činu) škola kontaktuje Policii ČR a Orgán sociálně-právní ochrany dětí.
- Škola informuje zasažené žáky o výsledcích šetření ve škole a udělených trestech.

## **Příloha č.5**

### **Jak uchovat důkazy kyberšikany?**

**Používejte Google** ([www.google.cz](http://www.google.cz)): v případě, že máte podezření nebo již zajišťujete důkazy ke kyberšikaně, **napište do okénka vyhledávače (Googlu) např. jméno oběti** či jinou indicii a uvidíte, zda se na internetu ještě něco dalšího najde.

### **Klávesové zkratky**

**Klávesa Print screen (Print Scrn):** tato klávesa „vyfotí“ aktuální zobrazení obrazovky, které následně uložíte v programu Word, malování, apod pomocí klávesy Ctrl V.

**Ctrl C (copy) a Ctrl V (vložit):** klávesové zkratky pro kopírování a vložení. Např. pokud vyfotíme pomocí klávesy Print scrn obsah nějaké stránky, tak pomocí Ctrl V vložíme tuto fotku např. do MS Word, Windows Malování apod..

**Ctrl A (all - vše):** označí vše a pak je možné obsah kopírovat pomocí Ctrl C

**Ctrl F (find - hledat):** po zmáčknutí se otevře okénko, do kterého můžete napsat jakékoli slovo a počítač ho automaticky vyhledá.

**Ctrl P (print - tisk):** pomocí této stránky vytisknete aktuální zobrazení obrazovky.

**Adresa – odkaz:** v každém prohlížeči je podlouhlé okénko, kde se zobrazuje aktuální **www adresa** dané stránky (např. www.seznam.cz). Je vždy umístěné zhruba 1 – 2 cm od shora obrazovky a je součástí ovládací nástrojové lišty prohlížeče (např. E-exploreru). Opět je možné i tuto adresu zkopírovat a uložit.

Obecné:

**Mobil:** V případech, kdy se kyberšikana odehrála prostřednictvím mobilního telefonu, **kontaktujte mobilního operátora.**

**Internet:** V případech, kdy se kyberšikana odehrála prostřednictvím internetu, **kontaktujte a spolupracujte s jakýmkoli webovým prostředím**, kde ke kyberšikaně došlo (např. MySpace, Facebook, Youtube, Lidé...). Jejich zaměstnanci jsou zvyklí spolupracovat při řešení kyberšikany a mohou vám asistovat při odstranění závadného obsahu, shromažďování důkazů, nebo vám mohou poskytnout kontakt na někoho, kdo vám může pomoci.

**Příloha č.6**

**3.2. Chronologická posloupnost jednotlivých kroků řešení z pozice školy a oběti (a rodiče)**

<b>Z pozice školy (ŠMP, TU, ředitele, IT...)</b>	<b>Z pozice oběti (a rodiče)</b>
<p><b>Zajistěte ochranu oběti</b> Kontaktujte operátora mobilní sítě nebo zřizovatele www stránek, profilu...atd. (viz přílohy 4. a 5.)</p>	<p><b>Ukončete komunikaci</b> Nekomunikujte s útočníkem, nesnažte se ho žádným způsobem odradit od jeho počínání, nevyhrožujte, nemstěte se. Cílem útočníka je vyvolat v oběti reakci, ať už je jakákoli.</p>
<p><b>Zajistěte dostupné důkazy s podporou IT kolegy</b> (viz příloha 5.)</p>	<p><b>Blokujte útočníka</b> Zamezte útočníkovi přístup k vašemu účtu nebo telefonnímu číslu a je-li to v dané situaci možné, i k nástroji či službě, pomocí které své útoky realizuje (kontaktujte poskytovatele služby).</p>

	<p><b>Důkladně vyšetřete a žádejte odb. pomoc</b>  Vyšetřete všechny souvislosti se zjištěným incidentem. Zajistěte si podporu a pomoc externího pracovníka (IT expert, PPP, policie,...). Kontaktujte a spolupracujte s MySpace, Facebookem, nebo jakýmkoli jiným webovým prostředím, kde ke kyberšikaně došlo.</p>	<p><b>Oznamte útok, porad'te se s někým blízkým, vyhledejte pomoc</b>  Svěřte se blízké osobě. Pro uchování důkazů oslovte někoho, kdo má vyšší IT gramotnost. Kontaktujte školu a specializované instituce (PPP, policii, SVP, LD, intervenční služby specializující se na řešení kyberšikany, psychology apod.).</p>
	<p><b>Opatření</b>  Zvolte takové opatření a řešení, které je odpovídající závažnosti prohrěšku a důsledkům, které agresor způsobil.</p>	<p><b>Uchovejte důkazy</b>  Uchovejte a vystopujte veškeré důkazy kyberšikany (SMS zprávy, e-mailové zprávy, zprávy z chatu, uložte www stránky apod.). Na základě těchto důkazů může být proti útočníkovi či útočníkům zahájeno vyšetřování. (postup viz příloha).</p>
	<p><b>Informujte a poučte rodiče</b>  Informujte rodiče oběti i rodiče kyberagresora. Postup a zásady sdělování informací jsou stejné jako u „klasické šikany“ (např. NE konfrontace oběti a agresora).</p>	<p><b>Žádejte konečný verdikt</b>  Po prošetření celého případu trvejte na konečném stanovisku všech zainteresovaných institucí.</p>
	<p>Poučte rodiče o tom, koho mohou (je vhodné) kontaktovat (Policie ČR, OSPOD, PPP, právní zástupce atd.). Některé případy kyberšikany nespádají do kompetence školy.</p>	
	<p><b>Žádejte konečný verdikt a informace</b>  Při zapojení a následně celém prošetření případu trvejte na konečném stanovisku všech zainteresovaných institucí (PČR...) a dalších subjektů (rodiče).</p>	
	<p><b>Postihy</b>  Při postizích agresorů postupujte v souladu se Školním řádem a již vypracovaným krizovým plánem.</p>	