



OCHRANA OSOBNÍCH ÚDAJŮ A OSOBNOSTI

Metodický materiál pro pedagogické pracovníky

Národní centrum bezpečnějšího internetu
2012



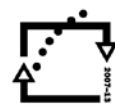
esf evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY

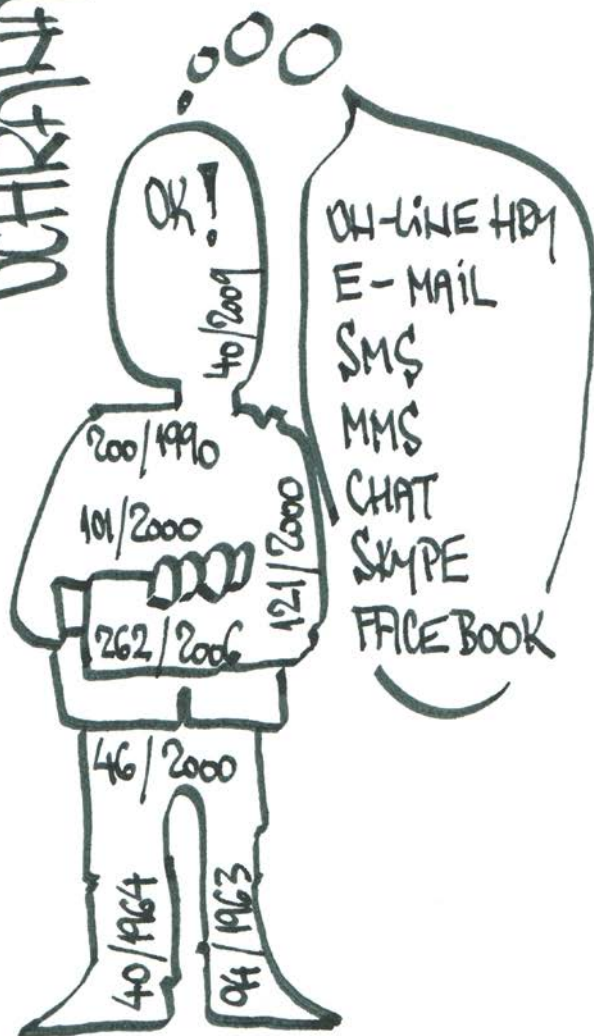


OP Vzdělávání
pro konkurenceschopnost

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

OCHRANA OSOBNÍCH ÚDAJŮ A OSOBNOSTI

METODICKÝ TEXT



OCHRANA OSOBNÍCH ÚDAJŮ A OSOBNOSTI PRAKTICKÁ PŘÍRUČKA

OCHRANA OSOBNÍCH ÚDAJŮ A OSOBNOSTI

Metodický materiál pro pedagogické pracovníky

Online bezpečí je především ochrana osobních údajů a dat

Rizika na internetu existují, jako v každé jiné oblasti lidské činnosti. A stejně jako jinde jim můžeme více či méně jít naproti. Při online komunikaci platí, že rizika zvyšujeme mnohonásobně, nejsme-li opatrní na své osobní a citlivé údaje a informace.

Děti a mladí lidé mají již lepší povědomí o tom, co jim na internetu může hrozit. Neumí se ale chránit a komunikovat bezpečně v praxi. Navíc mívají pocit, že jim kdesi přednášená rizika osobně nehrozí.

Hlavní důraz klade tento metodický materiál na fakt, že ochrana při online komunikaci znamená především ochranu svých osobních dat, citlivých a intimních informací a soukromí. Protože nic jako soukromí na internetu neexistuje, a to ani ve zdánlivě zabezpečených profilech.

Materiál Vás provede problematikou ochrany osobních a citlivých údajů a osobnosti na internetu a při online komunikaci. Pomůže Vám začlenit toto téma do výuky a podpořit tak bezpečí Vašich žáků.

Online komunikace

Dnešní dospívající komunikují především přes sociální sítě. Co je na sociálních sítích tak lákavé? Zejména to, že poskytují okamžité uspokojení potřeby společenského kontaktu.

Při moderní komunikaci je potřeba velmi pečlivě vážit kde, komu a co sdělujeme. Neboť osobní údaje a tzv. projevy osobní povahy jsou skutečnými klíči k našemu soukromí. Pokud je sdělujeme a zpřístupňujeme neuváženě, neopatrně nebo nevhodně, můžeme se dočkat nevyžádané, nečekané, nepřijemné nebo nevhodné odpovědi.

Přes veškeré právní normy a obecné snahy o co největší bezpečí internetového prostředí je to nakonec vždy otázka uživatelské volby, v jakém rozsahu poskytne informace o sobě samotném a v jakém rozsahu a k čemu toto prostředí použije nebo využije v něm nabízených služeb.

Rozlišení ochrany osobnosti a ochrany osobních údajů

Ochrana osobnosti a ochrana osobních údajů jsou dvě různé právní oblasti, které se mohou, ale nemusí vzájemně prolínat.

Stručně řečeno, ochrana osobnosti zahrnuje např. právo na soukromí a upravena je zejména občanským zákoníkem.

Oblast systematického zpracovávání osobních údajů upravuje zejména zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, který je doplněn řadou dílčích ustanovení v rámci jiných zákonů, upravujících např. povinnost archivace, evidence atp. Ochrana osobních údajů je součástí ochrany osobnosti, zakotvené v občanském zákoníku, osobní údaj může být součástí tzv. projevu osobní povahy.

Příklady ze školního prostředí

- Chcete-li na školním webu zveřejnit např. fotografie dětí ze školy v přírodě (na kterých jsou děti rozpoznatelné např. dle obličejů), v souladu s občanským zákoníkem tak nesmíte učinit proti jejich vůli, resp. proti vůli jejich zákonných zástupců.
- Chcete-li systematicky shromažďovat adresy přechodného pobytu dětí, musíte tak činit v souladu se zákonem o ochraně osobních údajů, neboť adresa je ve spojení s konkrétní osobou osobním údajem (škola má sice povinnost evidovat adresu trvalého pobytu dětí, ale přechodného nikoliv).
- Chcete-li však systematicky zveřejňovat fotografie dětí (např. umístit na web fotografie každého žáka, zvláště pak ve spojení s dalšími údaji, zejména příjmením), musíte tak učinit v souladu s občanským zákoníkem (vztahuje se na pořízení a zveřejnění fotografie jakožto projevu osobní povahy), ale zároveň i zákonem o ochraně osobních údajů (vzhledem k systematickosti).

Co je to osobnost z pohledu práva

Osobnost z pohledu práva zahrnuje aspekty fyzické, psychické, sociální i morální. Občanský zákoník chrání zejména život, zdraví, důstojnost, čest, vážnost, soukromí, jméno a projev osobní povahy, ovšem chráněny jsou i jiné hodnoty ryze osobní povahy, např. pseudonym, právo na identitu a osobní rozvoj. Součástí projevu osobní povahy může být např. záznam hlasu, nebo i osobní údaj (např. portrétní fotografie). Způsob nakládání s osobními údaji blíže vymezuje zákon o ochraně osobních údajů.

Kde je upravena ochrana osobnosti v zákoně

Nejvýznamnějším právním předpisem v oblasti ochrany osobnosti, který doplňuje obecný rámec ochrany poskytované Ústavou a Listinou základních práv a svobod, je občanský zákoník (zák. č. 40/1964 Sb., občanský zákoník, resp. zák. č. 89/2012 Sb., občanský zákoník). Dílčí úpravy pak najdeme např. v autorském zákoně (zák. č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů), zákoně o rodině (zák. č. 94/1963 Sb., o rodině), zákoníku práce (zák. č. 262/2006 Sb., zákoník práce), tiskovém zákoně (zák. č. 46/2000 Sb., o právech a povinnostech při vydávání periodického tisku a o změně některých dalších zákonů), zákoně o přestupcích (zák. č. 200/1990 Sb., o přestupcích), trestním zákoníku (zák. č. 40/2009 Sb., trestní zákoník) aj.

Ochrana osobnosti vlastní i druhých lidí

Každý člověk má právo na ochranu jeho osobnosti, vč. projevů osobní povahy. Z toho důvodu je možné pořídit jeho fotografický, zvukový nebo filmový záznam pouze s jeho svolením. To nemusí být výslovné, stačí svolení mlčky – např. tím, že nahrávaná osoba o nahrávání ví a neprotestuje proti němu (to platí i pro rozšiřování zobrazené podoby). Kromě toho nelze bez svolení dotyčného nebo bez zákonného důvodu sledovat jeho soukromý život nebo pořizovat o něm záznam. Svolení lze ovšem kdykoliv odvolat.

Pořídit nebo i použít záznamy osobní povahy je bez svolení dotyčné osoby možné jedine pro účely ochrany práv jiných osob, dále pak pro účely vědecké, umělecké nebo zpravodajské, ovšem i v těchto případech jen přiměřeně a tak, aby to nebylo v rozporu s oprávněnými zájmy dané osoby (např. nesmí to nepřiměřeně narušovat její důstojnost). Záznamy osobní povahy lze bez souhlasu dotyčné osoby použít také na základě zákona k úředním účelům.

Youtube

You Tube je server pro sdílení videí provozovaný společností Google, velmi oblíbený mezi mladými uživateli internetu. Tato platforma je často používána i pro zveřejňování a šíření násilných či ponižujících videí. Nahrávky pořízené a zveřejněné bez souhlasu zobrazeného porušují jeho právo na ochranu osobnosti. Je tedy oprávněn požadovat odstranění takového materiálu po tom, kdo jej umístil. Server umožňuje uživatelům nahlásit konkrétní obsah jako nevhodný a dožadovat se jeho smazání.

Odpovědnost za porušení práva na ochranu osobnosti

Občanský zákoník zakotvuje ochranu osobnosti každé fyzické osoby a názvu a dobré pověsti právnické osoby. Odpovědný za porušení práva na ochranu osobnosti (např. zveřejňováním nepravdivých údajů o jiném na sociálních sítích) může být i nezletilý. Odpovídá za způsobenou nemajetkovou újmu bez ohledu na její zavinění (např., i pokud zveřejní nepravdivé údaje, aniž by si byl jejich nepravdivosti vědom).

Dojde-li neoprávněným zásahem nezletilého do práva na ochranu osobnosti k majetkové škodě (např. ke vzniku vážné duševní poruchy u oběti vedoucí až ke ztížení společenského uplatnění), odpovídá za ni nezletilý, který je schopen ovládnout své jednání a posoudit jeho následky, a to společně a nerozdílně s tím, kdo byl povinen vykonávat nad ním dohled. Jestliže daný nezletilý není schopen ovládnout své jednání a posoudit jeho následky, odpovídá za škodu pouze ten, kdo nad ním je povinen vykonávat dohled. Osoba vykonávající dohled se může zprostit této odpovědnosti, jestliže prokáže, že dohled nezanedbala.

Jak se bránit při porušení práva na ochranu osobnosti

- Pokud někdo neoprávněně zasahuje do Vašeho práva na ochranu osobnosti, v první řadě vyjádřete svůj nesouhlas (např. se ohradte proti nahrávání).
- Jestliže jde o trvajících zásah (např. Vaše fotografie je proti Vaší vůli zveřejněna na webové stránce), požádejte autora o její smazání.
- Není-li to možné (např. autora neznáte nebo Vám odmítá vyhovět), požádejte o smazání s vysvětlením správce daného webu (tzv. poskytovatel služby má za jistých okolností odpovědnost za obsah v souladu se zák. č. 480/2004 Sb., o některých službách informační společnosti, a je proto i v jeho zájmu protiprávní obsah smazat).
- V případě, že neuspějete nebo Vám již byla způsobena majetková škoda nebo nemajetková újma, obraťte se na soud. Domáhat se můžete upuštěním od neoprávněných zásahů do práva na ochranu osobnosti (např. od opakovaného nahrávání Vašich projevů osobní povahy), odstranění jejich následků (např. smazání zesměšňujícího videa z webu), přiměřeného zadostiučinění (např. omluva), ve výjimečných případech i náhrady nemajetkové újmy v penězích.

Co jsou to osobní údaje

Osobní údaje jsou takové údaje, které jsou spojitelné s konkrétní osobou. Jedná se proto typicky např. o příjmení, adresu (vedoucí ke konkrétní osobě) nebo fotografii (na které lze danou osobu identifikovat). Tedy jakékoliv prvky specifické pro fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.

K osobním údajům patří i takové, které vedou ke konkrétní osobě až ve svém souhrnu (např. zaměstnavatel spravuje databázi osobních identifikačních čísel zaměstnanců a zároveň má přístup ke klíči, podle kterého lze na základě takového čísla identifikovat konkrétního zaměstnance).

Pod přísnější ochranou jsou citlivé údaje, tj. takové, které již vypovídají o dané osobě více (např. o rase, víře, sexuální orientaci, zdravotním stavu).

Právní úprava ochrany osobních údajů

Ochrana osobních údajů je zakotvena kromě Listiny základních práv a svobod a zákona o ochraně osobních údajů (zák. č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů) v řadě dalších zákonů. Jedná se např. o občanský zákoník (zák. č. 40/1964 Sb., občanský zákoník), obchodní zákoník (zák. č. 513/1991 Sb., obchodní zákoník), autorský zákon (zák. č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů), školský zákon (zák. č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání), zákon o přestupcích (zák. č. 200/1990 Sb., o přestupcích), trestní zákoník (zák. č. 40/2009 Sb., trestní zákoník) aj.

Úřad pro ochranu osobních údajů

Nad zpracováváním osobních údajů v souladu se zákonem o ochraně osobních údajů provádí dozor Úřad pro ochranu osobních údajů, který dále vede registr zpracování osobních údajů, poskytuje konzultace a svá stanoviska a v případě porušení povinností při zpracovávání osobních údajů ukládá nápravná opatření (vč. např. pokuty). Činí tak na základě plánu své dozorové činnosti nebo na základě podnětů zvenčí (lze se na něj proto obrátit s podezřením na neoprávněné nakládání s osobními údaji).

www.uoou.cz

Oprávnění ke shromažďování a nakládání s osobními údaji

Zpracovávání osobních údajů podléhá oznamovací povinnosti správce vůči Úřadu pro ochranu osobních údajů. Osobní údaje obvykle zpracovávají např. e-shopy nebo firmy poskytující různé služby na internetu. Je-li zpracování osobních údajů nezbytné pro plnění ze smlouvy (např. uchování adresy kupujícího do doby, než mu bude výrobek zaslán poštou), souhlas není nutný. Často je však pro dokončení objednávky nutné odsouhlasit širší rozsah zpracování osobních údajů, obvykle pro účely vedení databáze klientů. Mnohdy je v těchto podmínkách zakotven např. váš souhlas se shromážděním Vašich osobních údajů, možností použít je k marketingovým účelům tím, komu jste osobní údaje svěřili, možnost předat Vaše osobní údaje spřátelené organizaci atp. Každý by si měl přečíst, jakým způsobem bude s jeho údaji nakládáno (např. zda nedává souhlas i k předání svých osobních údajů další straně) a důkladně zvážit, do jaké míry je daný web nebo e-shop atp. důvěryhodný a zda poskytnutá služba nebo zboží stojí za poskytnutí osobních údajů.

Co dělat, není-li nakládáno s osobními údaji v souladu se zákonem?

Zákon o ochraně osobních údajů chrání každého před neoprávněným zasahováním do jeho soukromí při zpracovávání jeho osobních údajů, při jejich systematickém shromažďování, uchovávání, zveřejňování atp.

Domníváte-li se, že s Vašimi osobními údaji není řádně nakládáno (např. jsou osobní údaje nepřesné nebo uchovávány neoprávněně), požádejte správce či jejich zpracovatele o vysvětlení a případně o odstranění takového stavu (aby údaje např. opravil nebo smazal, doplnil, blokoval). Je-li Vaše žádost oprávněná, správce či zpracovatel jí vyhová a informuje Vás o tom. Pokud tak neučiní, obraťte se přímo na Úřad pro ochranu osobních údajů s konkrétní stížností či podnětem ke kontrole, žádoucí je pak v takovém případě zároveň zaslat Úřadu relevantní podklady k posouzení.

Právo být informován o nakládání s osobními údaji

Správce osobních údajů musí subjekt údajů informovat o jeho právu přístupu k osobním údajům, právu na opravu osobních údajů, jakož i o dalších právech stanovených v zákoně o ochraně osobních údajů. Taková informace může mít podobu např. všeobecných podmínek, s nimiž musíte vyslovit souhlas pro možnost využít nějakou službu (např. e-mailovou schránku), uskutečnit koupi v e-shopu atp.

Aktuální trendy v oblasti ochrany osobních údajů

Vzhledem k současnému věku informační společnosti lze předpokládat, že význam ochrany osobních údajů stále poroste, přinejmenším v členských státech EU. Evropská komise se v současnosti zaměřuje např. na úpravu pravidel ochrany osobních údajů s ohledem na globalizaci a používání nových technologií, na posílení práv jednotlivců a na zahrnutí řádné ochrany osobních údajů do všech oblastí aktivit EU.

Zneužití osobních údajů online

Kyberagresoři k uskutečnění svého záměru osobní údaje potřebují, ať už jim umožní dostat se k oběti samotné či třeba k jejímu majetku. Při tom často využívají údaje dobrovolně poskytnuté. Obzvláště citlivé údaje dávají útočníkovi do rukou velkou moc. Útočníci využívají různých "zbraní", jak potřebné osobní údaje získat.

Obohacení

Může jít např. o zneužití osobních údajů v majetkové oblasti (např. kombinace informace na FB o majetkových poměrech dotyčného ve spojení s jeho adresou a třeba zprávou o plánované cestě na dovolenou).

Psychické násilí

Osobní a citlivé údaje jsou zneužitelné i k nejrůznějším druhům psychického násilí. Dávají útočníkovi prostor pro manipulaci či vydírání. Velmi závažné je využití osobních údajů ke kyberstalkingu, kybergroomingu nebo kyberšikaně, kdy mohou sloužit jako „střelivo“ pro útočníka. Tak např. kyberstalker si se zájmem zjistí, jaké kroužky navštěvuje jeho oběť, aby si na ni mohl počkat. Kybergroomer si s chutí počte o tom, jaké koníčky má jeho oběť, pak snáze získá její přízeň. Kyberšikanující útočník využije s gustem každý peprný údaj, k jakému se dostane (dobře mu k tomu poslouží např. na internetu nalezená fotografie, kde náhodně zachycený dotyčný nevypadá zrovna nejlépe).

Krádež identity a podvody

Dalším příkladem je zneužití osobních údajů za účelem vydávání se za jiného, nejčastěji s cílem spáchání nějaké formy podvodu, ať už v rovině majetkové nebo osobní. Zde může fungovat efekt nabalující se sněhové koule: znalost pár osobních údajů pomůže získat o dotyčném další osobní údaje (např. se útočník může vydávat za blízkého příbuzného a žádat o další informace). Čím více toho o sobě člověk zveřejní, tím snazší může být vydávat se za něj, a to i dlouhou dobu bez jeho vědomí.

Cílená agresivní reklama

Velmi časté je také využití osobních údajů pro marketingové účely, zejména k cílené agresivní reklamě.

Techniky k “sosání” osobních údajů a jejich zneužití

Způsoby získávání různých údajů o uživatelích internetu jsou pestré a mnohdy velmi vynalézavé, souhrnně se nazývají sociálním inženýrstvím.

K těm nejčastějším způsobům patří **spyware** (monitorovací software), podvody ve stylu tzv. **nigerijských dopisů** (např. nabízení extrémně výhodných možností investic po zaplacení vstupního poplatku), **phishing** (e-maily z „důvěryhodného“ zdroje např. vyzývající k zadání údajů o uživateli na přiloženém odkazu), **pharming** (podvodné weby vydávající se za pravé, např. imitace vstupní stránky k elektronickému bankovníctví). Na sociálních sítích mohou být využíváni tzv. **boti** (software v tomto případě se tváří jako reálný uživatel a naprogramovaný k pokládání otázek jakoby při běžném hovoru).

Škola jako správce osobních údajů

Škola má ze zákona povinnost evidovat některé osobní údaje žáků (např. jméno a příjmení, rodné číslo, státní občanství, místo narození a trvalého pobytu, údaje o průběhu a výsledcích vzdělávání ve škole, některé zdravotní údaje aj.). Nad rámec povinné evidence může škola zpracovávat (např. shromáždit, zveřejnit atp.) osobní údaje žáků vesměs pouze s jejich souhlasem. U mladších žáků (obvykle mladších 15 let) je nutný souhlas jejich zákonných zástupců.

Nejčastější chyby při práci s osobními údaji žáků

I když škola nakládá s osobními údaji žáků řádně a s potřebnými souhlasy dětí či jejich rodičů, měla by i tak důkladně zvážit jejich zveřejňování na školním webu, zejména je-li přístupný pro kohokoliv. Zvláště zveřejňování fotografií dětí ve spojení s třídními rozvrhy může děti vystavit nebezpečí, že „si někdo na ně počká“.

Pro vymezení pravidel, s čím rodiče souhlasí a s čím ne, a také pro vlastní ochranu používají školy různá tzv. „Prohlášení rodičů/zákonných zástupců dítěte“. Jasně vyjádřený souhlas nebo nesouhlas rodiče/zákonného zástupce dítěte se zpracováním osobních údajů nebo zveřejňováním fotografií atp. je závazný nejen pro všechny zaměstnance školy, ale také pro další osoby, které jsou se školou v jakémkoli jiném pracovněprávním nebo dodavatelském vztahu.

Nejčastější chyby v „Prohlášení rodičů/zákonných zástupců dítěte“

- Příliš široké vymezení souhlasu. Např. „dávám souhlas ke zpracování osobních a citlivých údajů mého dítěte v souladu se zákonem o ochraně osobních údajů“ – zde chybí účel zpracování, jakých osobních údajů se souhlas týká a na jaké období.
- Nadbytečné vyžadování souhlasu tam, kde ho není třeba. Např. k uchování údaje o místu narození dítěte, který je ale součástí školní matriky (tu má škola povinnost vést, a tudíž k tomu souhlas nepotřebuje).

Čemu by se měly školy v „Prohlášení rodičů/zákonných zástupců dítěte“ raději vyhnout:

- Souhlas se zpracováním osobních údajů podle zákona o ochraně osobních údajů bývá smíchán spolu se souhlasem ke zveřejňování informací o dítěti a jeho fotografií podle občanského zákoníku (to samo o sobě není chybou, ale může být zdrojem nejasností).
- Souhlas ke zveřejňování informací o dítěti a jeho fotografií podle občanského zákoníku bývá formulován velmi široce a vágně (např. „souhlasím, aby byly zveřejňovány fotografie mého dítěte na internetových stránkách školy“) – vhodné je blíže upřesnit, o jaké fotografie se má jednat (aby měl rodič jistotu, že nepůjde např. o soukromé fotografie z dovolené).

Ochrana osobních údajů a osobnosti ze strany poskytovatelů internetových služeb

Přístup poskytovatelů internetových služeb k ochraně osobních údajů a osobnosti by měl odpovídat českým právním předpisům (včetně případného odstraňování závadného obsahu). V praxi se však ti největší, jako Youtube, Google, Facebook aj., řídí především svými interními pravidly, případně právním rámcem svých zahraničních sídel. Nesouhlasí-li uživatel s jejich přístupem, nezbyvá mu obvykle, než službu nevyužívat. Pokud zde někdo nalezne závadný obsah (např. porušení práva na ochranu osobnosti, neoprávněně zveřejněné osobní údaje, porušení autorského práva atp.), zpravidla je zdaleka nejrychlejší (a mnohdy i jedinou) cestou k jeho odstranění oznámení poskytovateli, že některé z jeho interních pravidel je porušeno. V takovém případě bývá reakce poměrně rychlá (na rozdíl od pouhého poukázání na porušení českého právního řádu).

Co Vás identifikuje ve světě online komunikace

Chování v online prostředí není tak anonymní, jak by se mohlo zdát. Každé zařízení přistupující k internetu má tzv. MAC a IP adresu, a ty lze za jistých okolností vystopovat (bohužel ne vždy). Zatímco MAC adresa umožňuje přístup k internetu jako takový (jde o adresu konkrétního síťového zařízení, tedy např. síťové karty v počítači), IP adresa dané zařízení v rámci sítě identifikuje např. jako konkrétní webovou stránku. Uživatelé nepomůže používání různých přezdivek atp., neboť může být identifikován podle takového zařízení (např. mobilní telefon). Pachatelé např. kyberšikany by si měli uvědomit, že jejich jednání je vystopovatelné.

Vyplňování osobních údajů v online aplikacích

S požadavkem na uvedení a odsouhlasení zpracování osobních údajů se na internetu setkáváme velmi často, při využití téměř jakékoliv služby, u e-mailové pošty, nakupování v e-shopech, využívání slevových portálů, registrace na sociální síti nebo chatu či na oblíbeném webu atp. Mnohdy bezmyšlenkovitě vyplníme jakýkoliv formulář, který je nám předložen, aniž bychom se zamysleli nad oprávněností provozovatele požadovat ty které osobní údaje.

Je-li zpracování jména, příjmení a adresy nezbytné pro plnění ze smlouvy, kde je jednou ze stran ten, kdo poskytl osobní údaje, jeho souhlas se zpracováním není nutný (i v těchto případech ale správce osobních údajů respektovat případný písemně vyjádřený nesouhlas se zpracováním osobních údajů). Typicky se jedná např. o potřebu e-shopu uchovávat adresu objednatele kvůli doručení zboží. Na druhou stranu pokud by chtěl daný e-shop adresy objednatelů zveřejňovat, už by k tomu potřeboval jejich souhlas.

Opatrně se svěřováním se

Pro bezpečné využívání internetu nestačí dbát na ochranu osobnosti a osobních údajů. Děti a zejména dospívající by měli být velmi obezřetní při sdělování různých intimností a poskytování jakéhokoliv citlivého materiálu přes internet vůbec (např. svěřením se s intimním problémem nebo posláním lechtivé fotografie). Jednají tak zpravidla dobrovolně, a nedochází proto k porušení jejich práva na ochranu osobnosti a nemusí být ani neoprávněně nakládáno s jejich osobními údaji, ale vystavují se velkému riziku zneužití takového materiálu. Platí rovnice, že čím intimnější materiál, tím větší riziko a horší dopady jeho zneužití.

Děti sdílné a důvěřivé

Ochota a potřeba vysílat do světa informace o sobě souvisí s věkem. Jedním z nejdůležitějších vývojových cílů v období dospívání je budování vlastní identity. Identitu si mladý člověk vytváří mimo jiné na základě zpětných vazeb okolí, především vrstevníků. Zpětné vazby jsou pro něj důležité, potřebuje je a snaží se je vyhledávat. Internet umožňuje nebývalým způsobem vlastní prezentaci a masivní zpětnou vazbu. Dospívající na internetu vyhledávají příležitosti ke komunikaci, prezentují se, budují nové vztahy, experimentují se sebeobrazem a ochotně jej vysílají do světa. Na jedné straně tak internet a s ním spojené komunikační nástroje pomáhají naplňovat přirozené potřeby mladých uživatelů. Na druhé straně se však ocitají ve zvýšeném ohrožení: ke komunikaci přistupují nenuceně, neohroženě, často až s naivní důvěrou. Ochotně poskytují osobní údaje, soukromé informace, fotografie. Experimentují se sexualitou, neváhají vyjadřovat nekonformní, až radikální postoje. Komunikují tady a teď, neřeší možné důsledky své nadměrné otevřenosti a sebeodhalení se v blízké či daleké budoucnosti.

Děti na internetu hledají oporu

- **emocionální**
přátelství, lásku, víru, empatii, hodnocení a zpětné vazby, na jejímž základě probíhá sebehodnocení a vytváření vlastní identity
- **informační**
informace a rady pomáhající řešit jejich aktuální problémy
- **instrumentální**
praktickou materiální pomoc (zapůjčení věci, zajištění vstupenek na koncert apod.)

Co by měly děti vědět

- Při práci s internetem respektují vlastní soukromí a chráním vlastní osobní údaje, chráním údaje svých blízkých.
- Při práci s internetem respektují soukromí druhých, nezveřejňují jejich údaje a chráním je ze stejného důvodu jako ty své.

Ale já to chci říct... online

Děti vstupují do rozhovorů, komunikují vzájemně, aby navázaly kontakt, získaly informace, utvrdily se ve svých postojích, vyzkoušely a ukázaly své dovednosti a jinak zapůsobily na druhé, opatřily si dodatkovou stimulaci, když se nudí a z mnoha dalších důvodů. Obsah komunikace může být více či méně důvěrný, přátelský i nepřátelský, emotivně podbarvený, racionální, kooperativní i konfliktní.

Při komunikaci tváří v tvář mají účastníci možnost měnit cíle, formu a obsah bezprostředně podle pozorovatelných zpětných vazeb komunikačního partnera (sdělený obsah, mimika, gesta, tón hlasu, postoj). U kyberprostorové komunikace je rejstřík zpětných vazeb omezen. Proto také varování o možném nebezpečí může být snadno přehlédnutelné nebo dokonce nezjistitelné. Při komunikaci tváří v tvář je většinou jasné, jaký typ komunikačního kanálu (bezpečný, potěšující, konfliktní, ohrožující, nadějný) a s kým se otevírá (matka, kamarád, příslušník jiného sportovního klubu, bezdomovec, Ježíšek).

Čím méně má dítě přátel v reálném světě, tím více touží po přátelích alespoň v kyberprostoru. Čím více dítě touží po kontaktu a odpovědi, tím více se stává neopatrnějším - sdělí o sobě i velmi intimní informace, protože očekává obdobné odpovědi.

Princip zvyšujících se rizik

Osamělý, separovaný uživatel

- + potřeba vztahu, komunikace
- + dostupná sociální síť
- + neinformovanost, neznalost
- + nezodpovědnost a ignorace rizik
- = **maximální ohrožení.**

Proč je přílišná sdílnost nebezpečná

Běžně používané sociální normy v reálném světě určují vcelku přesně, co je vhodné ukázat a co ne, co je vhodné sdělit a co ne. Obdobné platí i v kyberprostoru: přílišné sebeodhalení se, přílišná sdílnost nebo nevhodné sdělení může vyvolat nepříznivou reakci okolí. Znevažující, posměšný komentář, negativní hodnocení, pomluvu. To vše jsou útoky na identitu sdělujícího a většinou ho zraní.

Agresor může zaútočit impulzivně nebo plánovitě.

Při impulzivním útoku jednoduše využije situaci, kterou mu připraví nepoučený nebo neopatrný uživatel. Příkladem může být slečna nespokojená se svým zevnějškem, svým stylem života a se svou rodinou, která se na Facebooku svěří všem se svými starostmi, myšlenkami a pocity. Jakýkoli jiný náhodně přítomný uživatel může to, co si právě přečetl, použít k okamžitému útoku na neopatrnou slečnu, vysměje se jí, zkritizuje ji, pomluví a urazí. Situace se přenese z prostředí virtuálního do reality, pokud si celou výměnu přečte někdo, kdo slečnu osobně zná.

Plánovaný útok si agresor připravuje někdy i dlouhodobě. Sbírá intimní údaje, kompromitující fotografie nebo videa, vyvine často značné úsilí získat kontakty, adresy a nejrůznější informace nejen o vybrané oběti, ale také o jejích známých a rodině. Veškeré získané informace a materiály následně cíleně a systematicky použije proti nic netušící oběti.

Napadení oběti může mít podobu jednorázového útoku, příležitostně a nečekaně opakovaného útoku (i od jiné osoby – např. náhodného pozorovatele) nebo i systematického a dlouhodobého pronásledování

Útok může být realizován např. ve formě kyberšikany a šikany, kyberstalkingu a stalkingu, kybergroomingu nebo nejrůznějších jiných kyberhrozeb (např. krádež identity).

Neopatrně sdělovat osobní údaje je jako “dráždit hada bosou nohou” nebo “strkat tygrovi hlavu do tlamy!”

Několik příkladů, k čemu může dojít v důsledku přílišné sdílnosti:

Sdělení	Následek
Sdělení přílišného množství osobních údajů (pohromadě nebo i na různých zdrojích)	Vydávání se za dotyčného někým jiným. Ten pak snáze získá další údaje (vydává se např. za příbuzného), pod cizí identitou si půjčuje peníze atp.
Zveřejnění intimní fotografie	Znevažující nebo urážlivé komentáře, nejrůznější sexuální nabídky, útok kybergroomera, nekontrolovatelné šíření
Pochlubení se kvalitním vybavením bytu, „hlášení“ své momentální polohy na sociální síti	Pozvánka pro bytového zloděje
Sdělení tel. čísla, mailové adresy vlastní nebo členů rodiny	Obtěžování prostřednictvím nevhodných telefonátů, sms, mms, mailů, komentářů na sociálních sítích, pozvánka ke kyberšikaně
Sdělení adresy	Nezvaná a neohlášená návštěva, první krok ke stalkingu, zvýšené riziko nátlaku, vyhrožování či vydírání a jejich horší dopad
Sdělování intimních myšlenek a pocitů nebo třeba nedobrých školních výsledků	Nevyžádané, nevhodné, posměšné nebo urážlivé komentáře
Podrobný popis postavy, vlastní nespokojenosti s ní	Posměšné, znevažující nebo urážlivé komentáře
Zveřejňování nebo poskytování osobních údajů a údajů o preferencích zboží atp.	Cílená reklama, spam

Facebook – brána k informacím otevřená

Facebook může sloužit, stejně jako jiné sociální sítě, jako otevřené okno do soukromí jeho uživatele. Komu umožníme nahlédnout, záleží na nastavení soukromí, na ochotě zveřejnit ty které informace a na ochotě umožnit nahlédnutí výměnou za přístup k různým aplikacím (např. umožnění přístupu k údajům spojeným s profilem výměnou za možnost zaslání speciálního přání k Vánocům jinému uživateli atp.).

Pečlivě bychom proto měli vážit, jaké informace se mohou zobrazit v našem profilu uživatele. Nebezpečné je uvádění osobních a citlivých údajů v otevřeném profilu, profilu viditelném pro jakéhokoliv uživatele internetu. Velké opatrnosti je také třeba dbát při komunikaci s osobami známými pouze z virtuálního prostředí.

Pamatujte, že ani při nejsoukroměji nastaveném profilu na sociální síti není soukromí zaručeno!

Soukromé pasti

I při opatrném nakládání s osobními a citlivými údaji nás mohou zaskočit různé "pasti". Např. příspěvky námi vložené na tzv. zeď mohou vidět ostatní osoby v závislosti na nastavení soukromí našich přátel (uživatel na svou zeď zapisuje různé myšlenky, vkládá odkazy na zajímavé weby, fotografie atp. Vše, co na zeď vloží, zobrazí se zároveň na zdi jeho facebookových "přátel"). V tom případě už pak nemáme přímý vliv na to, kdo má k našemu příspěvku přístup. Stejně tak je to s našimi příspěvky, které někdo z našich přátel nasdílí.

Vhodné je také zvážit používání různých aplikací a her, které Facebook svým uživatelům nabízí. Zpravidla tyto služby slouží především k více či méně skrytému sběru informací o jejich uživatelích. Ty mohou být následně využity např. k cílené reklamě nebo poskytnuty za úplatu dalším stranám. Lze se setkat i s tzv. botem, tj. profilem řízeným počítačem, který se vydává za reálnou osobu s cílem získat o uživateli co nejvíce informací.

Nastavení soukromí na Facebooku

Přesto by při ochraně našich údajů mělo být prvním krokem nastavení soukromí.

Tzv. nastavení soukromí znamená, že si uživatel zvolí, co z jeho profilu může být zobrazováno a kým. Na prvním místě je pečlivé zvážení udávání vlastních osobních údajů při zřizování profilu (např. celé jméno, škola, bydliště, zaměstnavatel, heslo k e-mailu pro automatické stažení kontaktů Facebookem).

Kdykoliv později si lze zvolit, aby obsah související s vlastním profilem byl viditelný

1. pro kohokoliv, 2. pro přátele přátel (myšleno „přátele“ na Facebooku), 3. jen pro vlastní facebookové přátele, 4. pro nikoho kromě uživatele samého.

Nastavit soukromí lze na Facebooku tak, že po přihlášení se k profilu vpravo na horní liště klikne uživatel na malý trojúhelník a zvolí možnost „Nastavení soukromí“.



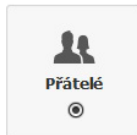
Dále dle vlastního uvážení zvolí jednotlivé možnosti např. v oblasti komunikace s ostatními, označování uživatele ostatními na fotografiích, poskytování informací aplikacím, hrám a webům.

Nastavení výchozího soukromí

Toto nastavení se bude vztahovat na aktualizace stavu a fotky, které zveřejníte na svém profilu prostřednictvím aplikace na Facebooku, jež není vybavena nástrojem pro interaktivní výběr uživatelů, jako je například Facebook pro Blackberry.



Veřejný



Přátelé



Vlastní nastavení

**Jak se spojujete**

Nastavte způsob spojení s lidmi, které znáte.

[Upravit nastavení](#)**Jak funguje označování**

Nastavte, co se stane, když přítel označí vás nebo váš obsah.

[Upravit nastavení](#)**Aplikace a webové stránky**

Nastavte, jaké údaje budete sdílet s aplikacemi, hrami a webovými stránkami.

[Upravit nastavení](#)**Omezení nastavení cílové skupiny uživatelů u minulých příspěvků**

Omezte viditelnost vašich příspěvků, které jste sdíleli s přáteli přátel nebo veřejností.

[Správa viditelnosti dřívějších příspěvků](#)**Blokování osob a aplikací**

Spravujte uživatele a aplikace, které jste zablokovali.

[Správa blokování](#)

Na tomto místě lze zároveň omezit viditelnost dřívějších příspěvků pouze pro přátele a především také v případě potřeby zablokovat obtěžujícího uživatele nebo aplikaci.

Vytvořte si vlastní nastavení soukromí ▶ Správa blokování

[◀ Zpět na nastavení soukromí](#)

Přidání přátel do seznamu Omezeno

Přidáte-li přítele do seznamu Omezeno, zobrazí se mu pouze informace a příspěvky, které nastavíte jako veřejné. Facebook vaše přátele neupozorní na to, že byli přidáni do seznamu Omezeno. Upravit seznam.

Zablokovat uživatele

Jakmile někoho zablokujete, tato osoba již pak nadále nebude vaším přítelem na Facebooku ani s vámi nebude moci komunikovat (kromě aplikací a her, které oba používáte, nebo skupin, v nichž jste oba členy).



Jméno:
E-mail:

Do seznamu blokovanych jste nikoho nepridali.

Zablokovat pozvánky aplikací

Po zablokování pozvánek aplikací od nějakého přítele budou všechny budoucí žádosti aplikace od tohoto přítele automaticky ignorovány. Chcete-li zablokovat pozvánky od konkrétního přítele, klikněte na odkaz „Ignorovat všechny pozvánky od tohoto přítele“, který se nachází pod nejnovější žádostí.

Blokovat pozvánky od uživatele:

Nezablokovali jste žádné pozvánky.

Zablokovat pozvánky na události

Poté, co zablokujete pozvánky od určité osoby, budou veškeré budoucí pozvánky od daného člověka automaticky ignorovány.

Blokovat pozvánky od:

Nezablokovali jste žádné pozvánky na události.

Způsob nastavení soukromí se sice čas od času mění podle rozvoje Facebooku, ale princip zůstává stejný. Pokud se Vám tedy nedaří soukromí nastavit, pravděpodobně to neznamená, že to nelze. Požádejte proto o radu zdatnějšího uživatele.

Souhlas ke zveřejnění obrázků a dalších osobních údajů samotnými dětmi

Svolení ke zveřejnění obrázků aj. osobních údajů je tzv. právním úkonem. Ten je neplatný, jestliže ten, kdo ho učinil, nemá způsobilost k právním úkonům. Plná způsobilost k právním úkonům vzniká zletilostí, nezletilí jsou do té doby způsobilí pouze k těm právním úkonům, které jsou přiměřené jejich rozumové a volní vyspělosti (v úvahu přichází věk nezletilého a např. jeho schopnost posoudit dopad rozhodnutí).

Je tedy namístě zvážit konkrétní vyspělost dítěte s ohledem na konkrétní právní úkon, který činí. Není-li pro udělení souhlasu dostatečně vyspělé, jako by jej vůbec nedalo (např. dítě v 11 letech pravděpodobně bude moci nakoupit v obchodě potraviny nebo dát souhlas ke zveřejnění svého křestního jména, ale nebude moci zakoupit nemovitost bez svého zákonného zástupce). Namísto nezletilého může dát souhlas k právnímu úkonu jeho zákonný zástupce (resp. souhlas zákonného zástupce je vždy nezbytný, není-li nezletilý k jeho udělení dostatečně rozumově a volně vyspělý). Např. zveřejnění fotografie dítěte mladšího 15 let se jménem bude obvykle možné pouze na základě souhlasu jeho zákonného zástupce. U starších dětí již může stačit souhlas zobrazených osob, je však třeba posoudit to vždy s ohledem na konkrétní dítě. Nejste-li si jisti, požádejte o souhlas zákonného zástupce dítěte.

Pedagogické zpracování

Děti by měly vědět, že to, co sdělím druhým o sobě a co sdělím druhým o druhých, má vždy své důsledky. Pokud si uživatelé internetu nedovedou nastavit a dodržovat komunikační hranice, potom riskují zranění. Přílišná otevřenost nebo nevhodné online vyjadřování mohou být příčinou takových zranění.

V rámci prevence rizikových jevů je vhodné dětem vštěpovat, že:

- základem veškerého mezilidského dění je komunikace,
- dobře vedená komunikace je základem dobrých a kvalitních vztahů,
- kvalitní vztahy se vytvářejí obtížně, ale velmi lehce se ničí,
- druzí jsou stejně důležití jako my,
- nečíň druhým to, co nechceš, aby bylo činěno tobě.

A na internetu:

- druhým sděluj pouze to, co je pro tebe skutečně bezpečné, co tě nemůže zranit nebo ohrozit,
- pečlivě zvažuj, komu dáš svou důvěru,
- nevíš, kdo se ke Tvým sdělením může dostat a jak je může proti Tobě použít,
- je nutné svou internetovou komunikaci chránit všemi dostupnými prostředky.

Je vhodné zvyšovat právní povědomí dětí tím, že je opakovaně věnována pozornost tématům:

- osobnost a osobní údaje z pohledu práva,
- osobnost a osobní údaje v rámci mezilidských vztahů,
- ochrana osobních údajů a osobnosti mé i druhých lidí,
- zneužití osobních údajů online,
- možnosti obrany při porušení práva na ochranu osobnosti a při neoprávněném nakládání s osobními údaji,
- odpovědnost za porušení ochrany osobnosti.

Ve školním prostředí jsou zjednodušené a vzájemně provázané výchovně vzdělávací působení a prevence dobře realizovatelné využíváním mezipředmětových vztahů (čeština - rodinná výchova, biologie - základy společenských věd, čeština - základy společenských věd, informatika - rodinná výchova aj.)

Slovníček pojmů

- **správce** podle zákona o ochraně osobních údajů = ten, kdo určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj
- **zpracovatel** podle zákona o ochraně osobních údajů = ten, kdo na základě zákona nebo pověření správcem zpracovává osobní údaje
- **subjekt údajů** podle zákona o ochraně osobních údajů = ten, ke komu se osobní údaje vztahují
- **zpracování** osobních údajů = zejména jejich shromažďování, ukládání, zpřístupňování, úprava, pozměňování, vyhledávání, používání, předávání dalším osobám, šíření, zveřejňování, uchovávání, výměna, třídění, kombinování, blokování, ale i likvidace

Pracovní listy

Výuková opora pro pedagogické pracovníky

Pracovní listy jsou součástí metodického materiálu

Pracovní list č. 1
1. stupeň ZŠ
BEZPEČNÉ A NEBEZPEČNÉ INFORMACE

Cíl činnosti:

Rozvoj dovedností pro bezpečné nakládání s osobními údaji a informacemi v online prostředí. Naučit se sdělovat o sobě, svých blízkých, kamarádech a přátelích pouze bezpečné, neohrožující informace.

Časová dotace:

45 min, práce celého třídního kolektivu

Pomůcky:

Na papíře formátu A2 velká barevná kresba semaforu, karty s osobními údaji a informacemi (zde příklad, pedagog si může připravit jiné karty dle vlastního uvážení, potřeby):

Karty s osobními údaji a informacemi:

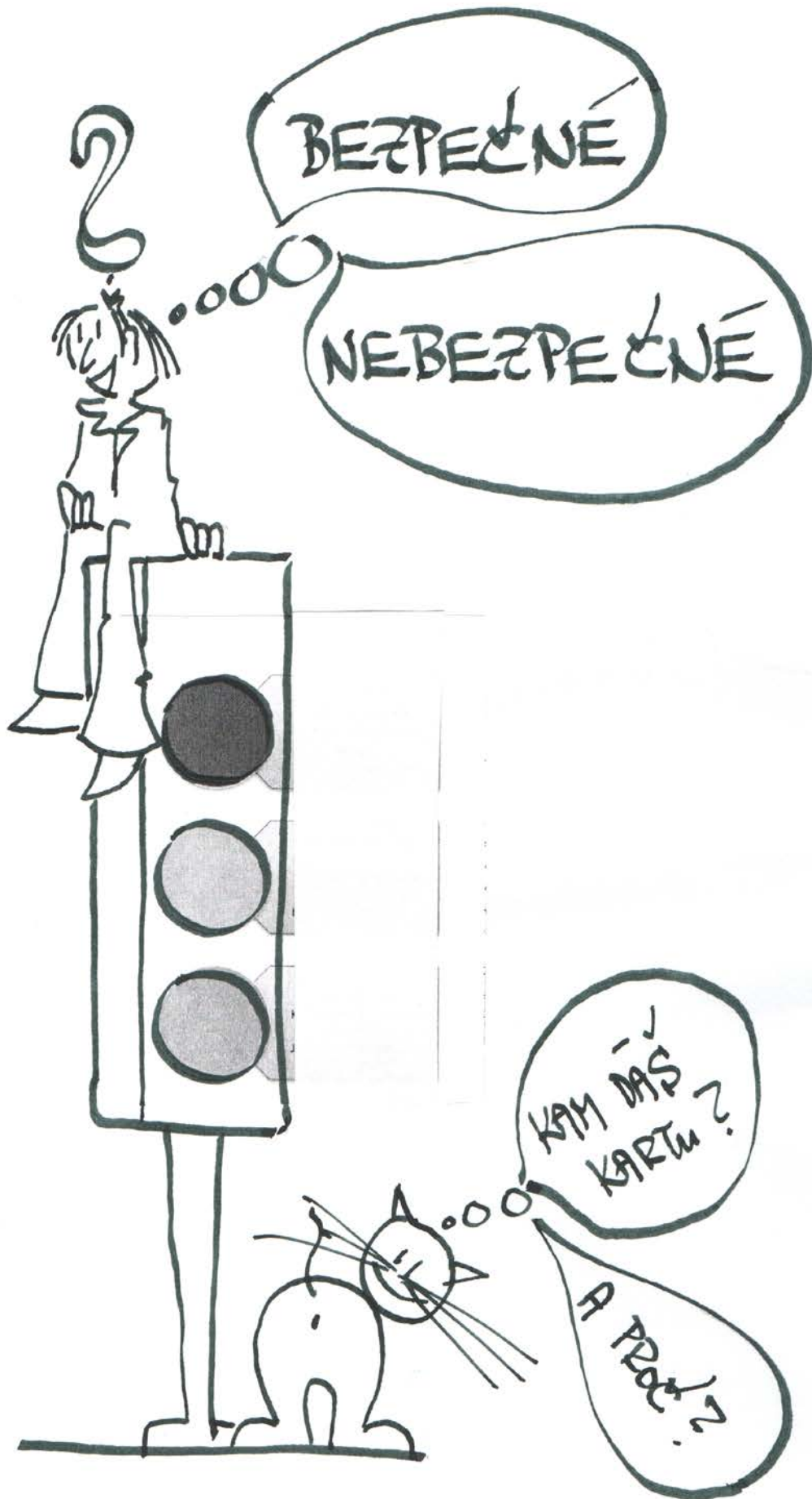
- křestní jméno
- vlastní fotografie
- věk
- popis vybavení bytu
- mailové heslo
- adresa kamaráda
- video z třídy o přestávce
- číslo na mobil
- příjmení
- jméno a příjmení
- příjmení a třída
- adresa bydliště
- jméno školy
- adresa školy
- rodné číslo
- fotografie celé rodiny
- fotografie sestry v plavkách
- stížnosti, jak mi rodiče nerozumí
- pracoviště rodičů
- nadávky
- pomluvy
- video z výuky

Průběh:

Karty s údaji jsou obráceny rubem vzhůru, žáci si postupně vybírají kartu z balíčku a přiřkládají ji ke světlu semaforu:

- **červená** nesmím sdělovat
- **oranžová** obecně lépe nesdělovat, když tak pouze důvěryhodným osobám
- **zelená** mohu sdělovat bez obav z ohrožení

Ke každé kartě je vedena diskuse, proč žák umístil kartu daným způsobem (zdůvodnění nebezpečí, příklady důsledků).



Pracovní list č. 2
1. stupeň ZŠ
NA INTERNETU NEMOHU VŠE, CO SE MI ZLÍBÍ

Cíl činnosti:

Povědomí o bezpečné a etické online komunikaci a ochraně osobních údajů a soukromých informací.

Časová dotace:

45 min, práce celé třídy v řízené diskusi

Pomůcky:

Balící papír

Průběh:

Za domácí úkol žáci napíší alespoň 3 body „Co bych neměl/a uvádět na internetu“. Uvedené body krátce zdůvodní.

Body žáci přednesou a společně zapíší na tabuli či list balícího papíru.

V řízené diskusi pedagog pracuje s tématy:

- jaké máme k dispozici komunikační nástroje
- proč je přílišná sdílnost nebezpečná
- jaké údaje mohou být zneužitelné a ohrožující, pokud je zveřejníme na internetu
- je možné mít na internetu soukromí
- nechráníme pouze sebe, ale také údaje a soukromí druhých
- jak chápeme osobnost a osobní údaje
- odpovědnost autora za zveřejněné údaje
- možné následky zveřejnění ohrožujících údajů

Poznámka:

Za vhodné považujeme zvolit méně formální uspořádání než v lavicích, např. sezení v kruhu, na koberci apod.

Pracovní list č. 3
1. stupeň ZŠ
RIZIKA PŘÍLIŠNÉ OTEVŘENOSTI

Cíl činnosti:

Uvědomění si, že z kyberprostoru může snadno a rychle přijít ohrožení nebo útok. Zejména, pokud mu samotný uživatel ulehčí práci sdělením osobních a citlivých údajů.

Časová dotace:

45 min, z toho 30 min práce jednotlivců, 15 min společná diskuse

Pomůcky:

Předtištěná grafická předloha s tabulkou, psací potřeby, pastelky

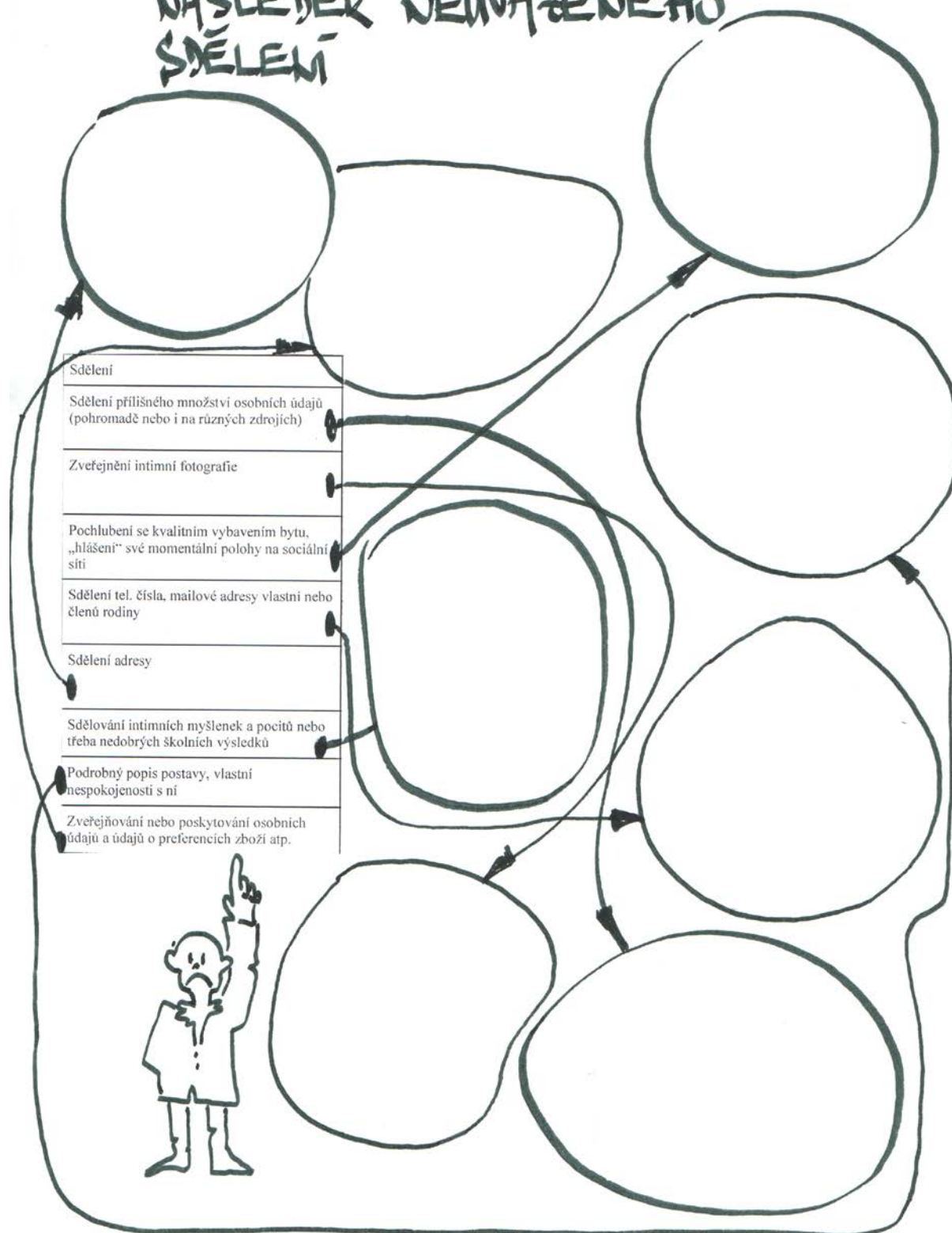
Průběh:

Žáci dokreslí a dopíší předtištěnou grafickou předlohu.

V tabulce je vždy uveden typ ohrožujícího sdělení. Žáci dle svého uvážení do bublin vpisují možný následek.

Následuje diskuse a opakování, které údaje na internet nepatří, co jsou tzv. Tabu údaje.

DO BUBLINI NAPIŠTE MOŽNÝ NÁSLEDEK NEUVÁŽENĚHO SDĚLENÍ



Pracovní list č. 4
2. stupeň ZŠ
JÁ, JAKO UŽIVATEL INTERNETU

Chovám se v kyberprostoru stejně jako v běžné 3D realitě?

Cíl činnosti:

Sebereflexe žáka a jeho chování v běžném životě/realitě a na internetu/sociální síti/facebooku.

Časová dotace:

2 x 45 min (dvouhodinovka), práce třídy, práce jednotlivců

Pomůcky:

Linkovaný papír formátu A4 vertikálně rozdělený na 2 poloviny nadepsané
Mé chování v životě – Mé chování na internetu, psací potřeby.

Na tabuli možná nápověda:

- Používám stejná slova ve třídě i na Facebooku?
- Svěřuji svá tajemství nebo na internetu?
- Jsem opatrnější na internetu než mezi známými a kamarády?
- Mám strach z neznámých lidí z internetu?
- Mám pocit, že se lépe seznamuje venku nebo na internetu?
- Myslím si, že je snadnější pomlouvat, lhát...na internetu?
- Mám větší zábrany při komunikaci tváří v tvář nebo na internetu?

Nápovědu si pedagog upravuje na základě vlastních znalostí komunikační úrovně a chování tříd.

Průběh:

1. hodina

Práci s tímto pracovním listem by měla předcházet volná diskuse na téma chování tváří v tvář a online.

2. hodina

Práce jednotlivců s pracovním listem (cca 30 min), sdělování postřehů o zjištěných rozdílech v chování.

Poznámka:

Dají se očekávat nejrůznější sdělení, postřehy zpětné vazby neboť pohled jednotlivce na sebe sama se nemusí shodovat s pohledem ostatních. Pokud by k takovýmto masovějším reakcím došlo, doporučujeme zvážit, zda nebude vhodné zařadit další hodinu, která se bude věnovat pouze diskusí o zjištěných rozdílech.

Pracovní list č. 5
2. stupeň ZŠ
JSEM MLUVKA, NO A CO

Všechno co vím, vykecám, co nevím to si vymyslím, pomluvím každého
a ještě se u toho dobře bavím!

Cíl činnosti:

Svobodná a otevřená reflexe žáků k příběhu, nezáleží, zda souhlasná či odsuzující, důležitým by měl být závěr, že za obsah uveřejněných věcí na internetu vždy zodpovídá autor.

Časová dotace:

45 min, z toho 20 min práce jednotlivců s příběhem, 25 min předčítání komentářů jednotlivců a společného vyvození poučení/závěru/návodu ...

Pomůcky:

předtištěný příběh a grafická předloha, psací potřeby, pastelky

Průběh:

Žáci pracují dle uvedených pokynů s grafickou přílohou a příběhem. Dokreslují, dopisují a komentují dle vlastního uvážení podle níže uvedeného příběhu. Každý podle svých vlastních názorů, pocitů, představ příběh písemně komentuje.

„Je mi 14, jsem skejťák, holky se mi líbí a já jim taky...Mám spoustu kámošů a na netu mnoho přátel. Každý den jsem on-line tak tři, čtyři hod'ky. Hraju hry, skypuji, píši si s přáteli. Fotr chce abych cvičil matiku a čedinu, ale na to já kašlu, kámoš mi pošle hotová cvičení a já mu je ukáži. Dycky na to skočí. A pak dá pár pěttek na nový triko nebo tak. Do značkových věcí se moc nehřnu, není třeba. Ne jako holky z třídy, nová řasenka, značková rtěnka, nejdražší podprda, furt kecy o tom kde maj jaký slevy. Blbiny. Mám super chytřej mobil, super nočas a perfektní prkno. Škola nic moc, ale s učama to koulím dobře. Důležité je dycky vědět o všem a každém všechno. Sbírám informace kde jen můžu. A lidi povídají rádi. Dozvídám se spoustu věcí, někdy jsou to pěkný ptákoviny, někdy vyložený hovadiny, někdy se tomu i dá věřit. Všecko pouštím dál, když to není moc in, tak to přibarvím. A pak koukám co z toho vyleze. Je to supéééééééér!!“



Předčítání komentářů.

Společná formulace závěru – společné myšlenky – napsat na tabuli.

Poznámka:

Časová dotace je pouze doporučená, pedagog si ji může upravit na základě znalosti pracovní výkonnosti jednotlivců a třídy.

MŮJ KOMENTÁŘ K PŘÍBĚHU:
MINIMÁLNĚ 50 SLOV

JSEM: 





DOKRESLI, VBARVI, NAPIŠ TAK
ABY SE VYSLEDEK CO NEJVIČE BUŤIL K PŘÍBĚHU

Pracovní list č. 6
2. stupeň ZŠ
KYBERPROSTOROVÝ KONDOM

Dostupné prostředky ochrany internetové komunikace.

Cíl činnosti:

Zvnitřnění/vštípení informace/faktu, že internet může být velmi nebezpečným prostředím, ze kterého může přijít napadení odkudkoli, kdykoli a kýmkoli. Proto je nutné počítat si obezřetně a umět se vhodně chránit a bránit.

Časová dotace:

45 min, práce učitele s celou třídou jednotlivců

Pomůcky:

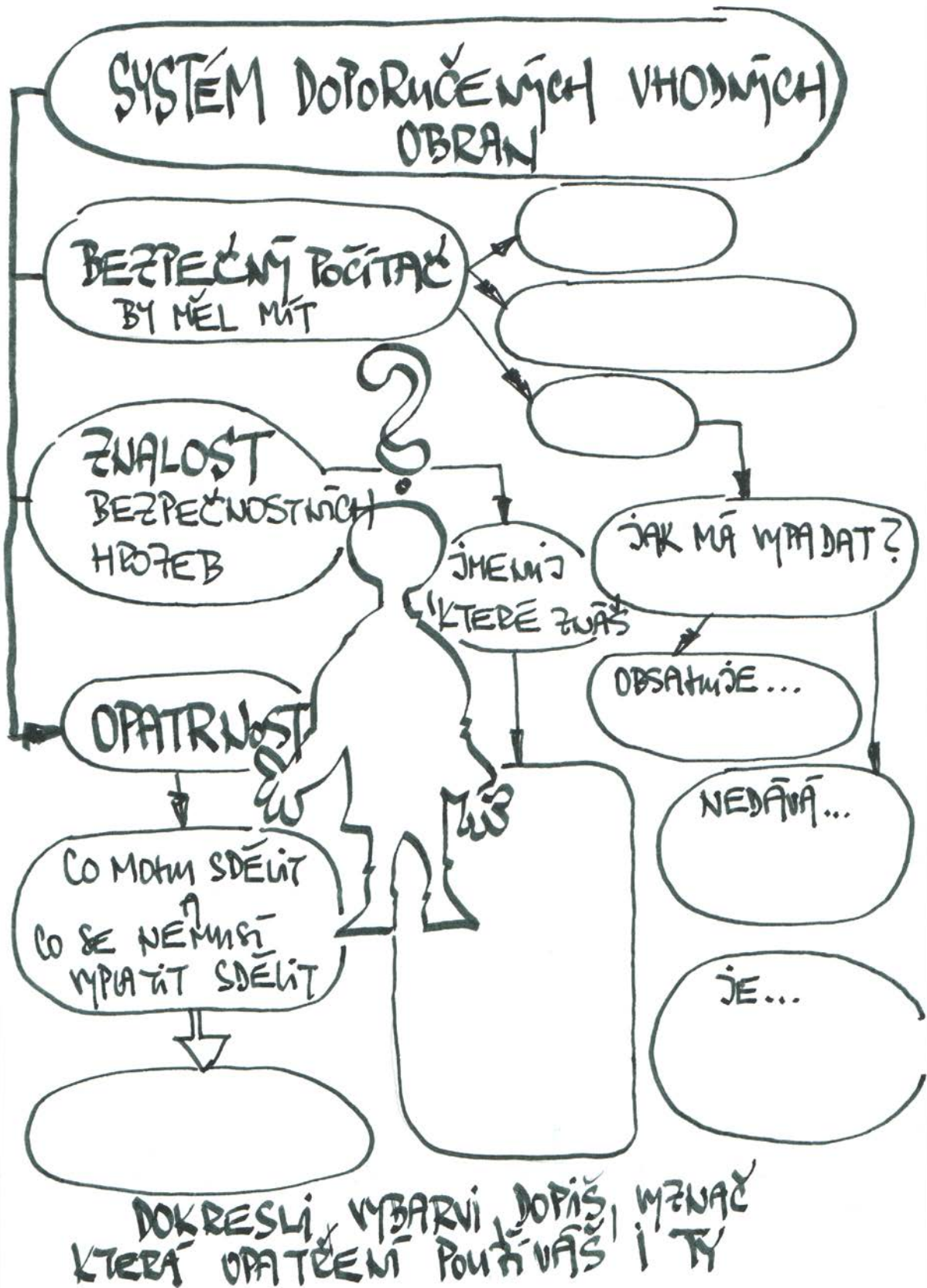
Předtištěná grafická příloha, pastelky, psací potřeby

Průběh:

Práci s tímto pracovním listem musí předcházet seznámení s pojmy:

- systém obran
- firewall (odděluje počítač od internetu a povoluje jen vyžádanou komunikaci)
- antivirový program (sleduje podezřelé aktivity, vyhledává neznámé programy, identifikuje známé viry)
- virus (malý program, který se umí vložit do jiného programu a s ním se šíří)
- heslo (by mělo obsahovat minimálně 8 různých znaků, dá se dobře zapamatovat, aby nebylo potřebné si je zapisovat, např. věta)
- bezpečnostní hrozba
- opatrnost v kyberprostorové komunikaci

Žáci samostatně doplní grafický list, dokreslí, dopíší. Pedagog v diskusi s celou třídou provádí kontrolu správnosti odpovědí.



Pracovní list č. 7

2. stupeň ZŠ

SOSÁNÍ

Cíl činnosti:

Procvičení vědomostí o různých typech možných ohrožení v důsledku zneužití osobních údajů.

Časová dotace:

45 min, práce jednotlivců

Pomůcky:

PC učebna, poznámkový list A4, psací potřeby

Průběh:

Žáci na samostatných pracovištích vyhledávají následující hesla, obsah zjištěného si zaznamenávají.

- sociální inženýrství
- phishing
- pharming
- spoofing
- spyware
- boti

Vyhledají alespoň dva skutečné příběhy, články, eseje, varování apod. pojednávající o příkladech zneužití osobních údajů. Vyhledaná fakta si přečtou a zaznamenají stránku, ze které čerpali.

Poznámka:

S tímto pracovním listem je možno pracovat „v sérii“ s jinými pracovními listy, které se zabývají prevencí před nebezpečími plynoucími z neopatrného užívání on-line technologií.

Pracovní list č. 8

3. stupeň SŠ

PŘÍLIŠNÁ SDÍLNOST

Na netu o sobě a všech řeknu vše? Co mne k tomu vede?

Cíl činnosti:

Procvičení vědomostí o různých typech možných ohrožení v důsledku zneužití osobních údajů.

Časová dotace:

45 min, práce jednotlivců

Pomůcky:

PC učebna, poznámkový list A4, psací potřeby

Cíl činnosti:

Sebereflexe vlastní otevřenosti a sdílnosti v kyberprostorové komunikaci.
Porovnání vlastního chování v kyberprostoru a v běžné realitě.

Časová dotace:

45 min, práce celé třídy

Pomůcky:

tištěný text, zjednodušený příběh

Průběh:

Diskuse k příběhu.

„Je mi 17, příští rok budu maturovat na gymplu. Měřím 170 cm, mám něco kolem 75 kilo, beďary mne netrápí. Nemyslím si, že bych vypadal špatně, oblékám se dobře, většinou do značkových věcí. Žádný lumen nebo šprt nejsem, ale ani ne nejloupejší. Jsem dobrý v maticce, docela dobře tančím, mám vlastní motorku, docela slušné počítačové vybavení. Nechodím často do hospody, z drog neznám nic. Jsem neviditelný. Ve třídě je hodně zamilovaných, několik párů, nějaká ta skupina sportovců, pár rádoby feťáků, pár sprayerů. Nepatřím nikam. Rodičové se zajímají o známky, a zda nepotřebuji peníze. Na netu trávím hodně času, mám hodně přátel na Facu, mailuji a skypuji i se spolužáky. Jsem otevřený a otevřenost očekávám i od ostatních. Dozvídám se spoustu věcí, někdy jsou to pěkné ptákoviny, někdy vyložené hovadiny, ale často i věci, se kterými souhlasím. Všechno pouštím dál, běžně připojuji vlastní komentář. Na netu jsem někdo, akorát, že jinak pořád zůstávám pro ostatní neviditelný.“

Názory a pocity studentů, reflexe k příběhu, vlastní sebereflexe o otevřenosti a sdílnosti v kyberprostorové komunikaci.

Pracovní list č. 9

3. stupeň SŠ

PRÁVNÍ ASPEKTY OCHRANY OSOBNÍCH ÚDAJŮ

Cíl činnosti:

Rozvoj právního povědomí studentů a základní orientace v zákonech souvisejících s ochranou osobních údajů a osobnosti.

Časová dotace:

Jedná se o rozsáhlý úkol, za vhodné považujeme realizovat jej formou projektu, např. týdenního nebo měsíčního.

Pomůcky:

dle potřeb projektu, základní pravděpodobně PC, velké papíry, barvy, lepidlo apod.

Průběh/opora pro plánování projektu:

1. Stanovení cíle projektu:
2. Pojmenování:
3. Naplánování realizace:
 - a. časový rozsah
 - b. jakou formou
4. Realizace by měla obsáhnout všechny zákony našeho právního systému zabývající se ochranou osobních údajů a osobnosti, tedy:
 - a. 94/1963 - Zákon o rodině
 - b. 40/1964 - Občanský zákoník
 - c. 200/1990 - Zákon o přestupcích
 - d. 46/2000 - Tiskový zákon
 - e. 101/2000 - Zákon o ochraně osobních údajů
 - f. 121/2000 - Autorský zákon
 - g. 262/2000 - Zákoník práce
 - h. 40/2009 - Trestní zákoník
5. Prezentace:
 - a. kdy
 - b. kde
 - c. kdo
 - d. před kým
 - e. jakou formou: plakát, slady power pointu, počítačová animace, hraná scénka apod.
6. Hodnocení:
 - a. samotnými realizátory
 - b. dohlížejícím/vedoucím pedagogem
 - c. účastníky prezentace (rodiče, vedení školy, jiná třída apod.)

Pracovní list č. 10
3. stupeň SŠ
MOC MLUVÍM, JE TO BEZPEČNÉ?

Cíl činnosti:

Budování zodpovědnosti za vlastní kyberprostorovou komunikaci. Za povahu, množství a obsah sděleného zodpovídá autor, nikoli poskytovatel připojení a datového prostoru. Kontrola znalostí k danému tématu.

Časová dotace:

45 min, práce jednotlivců

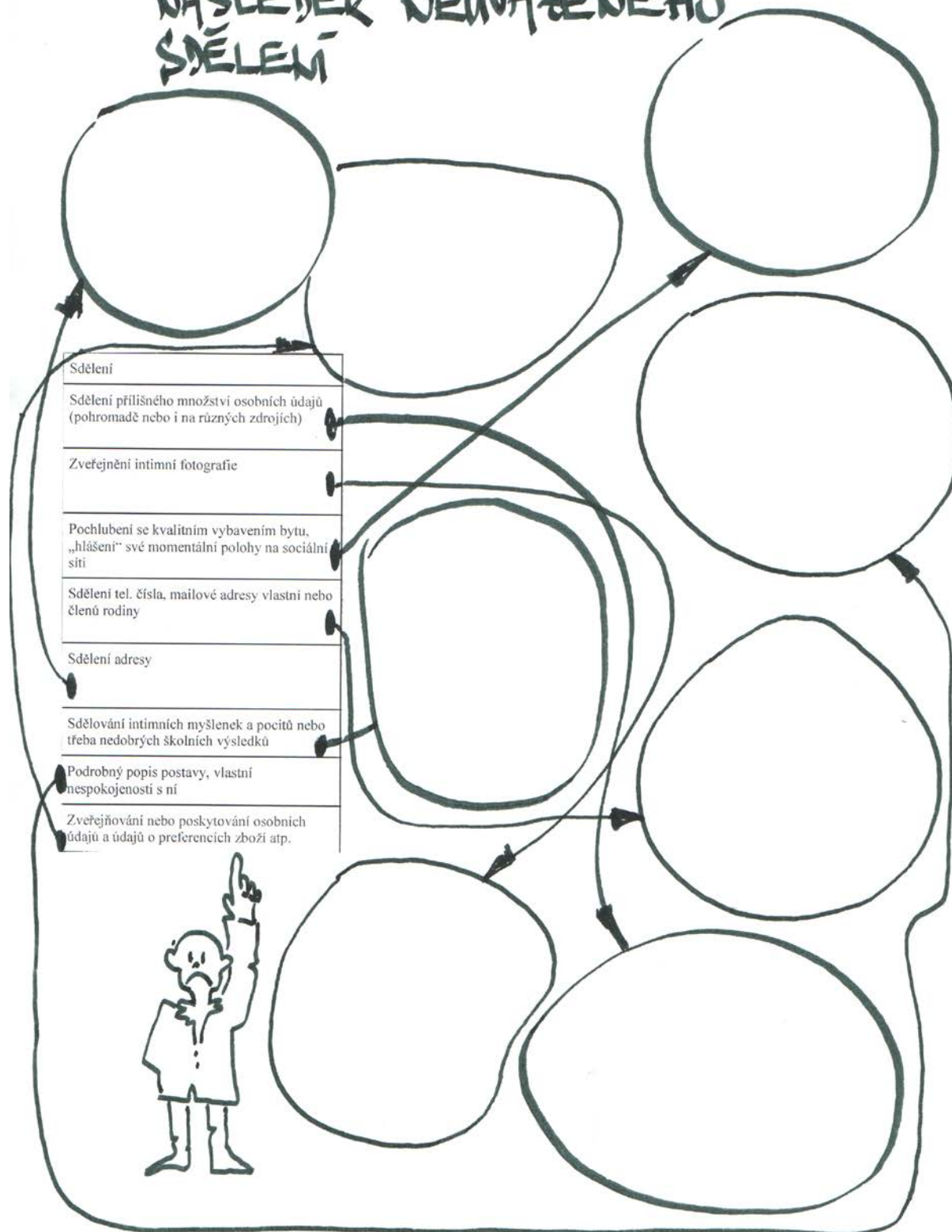
Pomůcky:

tabulka a grafická předloha

Průběh:

Studenti vyplňují předtištěnou grafickou předlohu. V tabulce je uveden typ ohrožujícího sdělení, do bublin vpisují možný následek.

DO BUBLINI NAPIŠTE MOŽNÉ NÁSLEDEK NEUVÁŽENĚHO SDĚLENÍ



Pracovní list č. 11

3. stupeň SŠ

ŠMÍROVÁNÍ

Cíl činnosti:

Neveřejná sebereflexe na téma šmírování, porušování soukromí druhých – porušení listovního tajemství, lustrace cizího mobilu, čtení cizí mailové pošty.

Časová dotace:

45 min

Pomůcky:

předtištěný, soukromý, přísně důvěrný otazníček, psací potřeby

Průběh:

Studenti odpovídají na otázky uvedené v dotazníku. Pedagog apeluje na co největší autenticitu a upřímnost odpovědí. Předem sdělí, že dotazník je soukromý, anonymní, nikde se s ním nebude dále pracovat.

1. Mám vlastní zkušenost s čtením cizí pošty: ano – ne
2. Když vidím cizí mobil, neodolám vábení prostudovat jej: ano – ne
3. Byl to mobil: sourozence – rodiče – přítele/kyně – kamaráda
4. Ze zjištěných informací jsem měl/a radost: ano – ne
5. Zjištěné informace jsem nějakým způsobem použil/a: ano – ne
6. Když se dostanu k cizímu PC heslu: použiji je – nepoužiji
7. Nestydím se hrabat v cizím soukromí: ano – ne
8. Nikdy mi nedošlo, že by se to nemělo: ano – ne
9. Při čtení soukromých informací jsem byl/a přistižen/a: ano – ne
10. Víím, že porušováním listovního tajemství, lustrací cizího mobilu, čtením cizích mailů se dopouštím trestného činu: ano – ne
11. Hrozí mi trest:
12. V budoucnosti, když budu mít příležitost, poruším soukromí druhých: ano – ne
13. Je to pro mne adrenalinový zážitek: ano – ne
14. Po vyplnění tohoto dotazníku se cítím:

Po vyplnění dotazníku, zodpovězení otázek dostanou čas zamyslet se nad svými odpověďmi. Potom jej dle vlastního rozhodnutí mohou zničit. Pokud budou mít studenti zájem, může tento pracovní list pokračovat diskusí nad zjištěnými výsledky.

Důležité online zdroje:

Link	Co zde najdu?
www.uoou.cz	Web Úřadu pro ochranu osobních údajů
www.ooou.cz	Ochrana osobních údajů stručně, web soukromé společnosti
http://ec.europa.eu/justice/data-protection/index_en.htm	Web Evropské komise k ochraně osobních údajů (AJ)

Doporučená literatura:

JUDr. MgA. Michal Šalamoun: "Ochrana osobních údajů v teorii i praxi, e-kniha"

W. Glasser, *Terapie realitou*, Portál, Praha 2001, ISBN 80-7178-493-1

M. Nakonečný, *Sociální psychologie*, Academia, Praha 1999, ISBN 80-200-0690-7

J. Výrost, I. Slaměník, *Aplikovaná sociální psychologie II*, Grada, Praha 2001, ISBN 80-247-0042-5

S. Covey, *7 návyků skvělých teenagerů*, Pragma, Praha 1998, ISBN 80-7205-799-5

Související právní předpisy:

Ústavní zákon č. 1/1993 Sb., Ústava České republiky

Ústavní zákon č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky (Listina základních práv a svobod)

Zákon č. 101/2000 Sb., o ochraně osobních údajů

Zákon č. 40/1964 Sb., občanský zákoník

Zákon č. 89/2012 Sb., občanský zákoník

Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon)

Zákon č. 94/1963 Sb., o rodině

Zákoník č. 262/2006 Sb., zákoník práce

Zákon č. 46/2000 Sb., o právech a povinnostech při vydávání periodického tisku a o změně některých dalších zákonů (tiskový zákon)

Zákon č. 200/1990 Sb., o přestupcích

Zákon č. 40/2009 Sb., trestní zákoník

Zákon č. 480/2004 Sb., o některých službách informační společnosti

Zákon č. 513/1991 Sb., obchodní zákoník

Zákon č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon)

Materiál vznikl v rámci projektu Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016.

Tento projekt je prostřednictvím Operačního programu Vzdělávání pro konkurenceschopnost financován z Evropského sociálního fondu a státního rozpočtu ČR.



Vydalo Národní centrum bezpečnějšího internetu v roce 2012.

Na materiálu spolupracovali Mgr. Anna Mašková, Mgr. Kateřina Lukášová, Mgr. Rastislav Pacák a Mgr. Jana Brandejsová.

www.saferinternet.cz

www.ncbi.cz

www.bezpecne-online.cz