TABLETY DO ŠKOL

– POMŮCKA PRO PEDAGOGA

VE SVĚTĚ DIGITÁLNÍHO VZDĚLÁVÁNÍ

Internet a zákony

BEZPEČNOST INTERNETU

ŠKOLA A ZÁKONY

ŘÁDY ODBORNÝCH UČEBEN

ŠKOLNÍ SÍŤ UMÍ DOTYKOVÁ ZAŘÍZENÍ

Příručka pro metodiky

Pavla Velecká

2014

esf evropský sociální fond v ČR

EVROPSKÁ UNIE

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

OP Vzdělávání pro konkurenceschopnost

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Název projektu: Tablety do škol - pomůcka pro pedagoga ve světě digitálního vzdělávání

Registrační číslo projektu: CZ.1.07/1.3.00/51.0002

Tento produkt je spolufinancován z Evropského sociálního fondu a státního rozpočtu České republiky.

Obsah

1 Úvod

Tato příručka se věnuje třem hlavním tématům. Prvním je bezpečnost internetu. V době kdy jsou školy vybavovány moderními technologiemi umožňujícími sofistikovanou komunikaci, sdílení dat, jednoduché umísťování textů, fotografií i videosouboru na internet, vzrůstá obrovským způsobem možnost jejich zneužití. Existuje několik významných druhů internetové kriminality nebo škodlivého chování, které je potřeba pojmenovat a snažit se mu předcházet. V ohrožení jsou nejen žáci, ale i učitelé. Pouze poučený pedagog je schopen rizikové jevy odhalit a problémy řešit.

Druhým tématem jsou důležité zákony a předpisy, které se nějakým způsobem dotýkají užívání IT technologií ve školách. Ať už se jedná o školský zákon, autorský zákon nebo vyhlášky o bezpečnosti práce či vnitřní směrnice a řády učeben ve školách.

Třetím tématem jsou právě řády odborných učeben, které by měly být v souladu se všemi nadřazenými předpisy a také by měly chránit uživatele i zařízení školy. Příručku uzavírá několik praktických příkladů týkajících se řádů počítačových učeben.

2 Bezpečnost při využívání internetu

2.1 Co je prospěšné, je i bezpečné?

Zásadním problémem internetu a IT technologií obecně je, že nebezpečí v nich skryté není na první pohled patrné. V podstatě tytéž důvody, proč jsou tyto moderní technologie nasazovány, bývají v některých situacích vnímány jako riziko nebo nebezpečí. Rychlý přístup k informacím, možnost jednoduše a rychle umísťovat na internet texty a obrázky, široká dostupnost připojení, obrovská dostupnost videí na internetu a jejich jednoduché umísťování na webové stránky – to jsou všechno skvělé vymoženosti, úžasný technologický pokrok, který lze výborně využít ku prospěchu žáků, vyučovacího procesu i samotného pedagoga. Ale každá hůlka má dva konce. Vše, co je možné využít pozitivně, je možné zneužít i k negativním cílům.

V této části se budeme věnovat odvrácené stránce internetu. Je dobré šířit mezi pedagogy osvětu a ukázat možná nebezpečí, která se za IT technologiemi mohou skrývat. Je pravdou, že běžný český pedagog není většinou přeborníkem v komunikaci na sociálních sítích a výpočetní techniku používá sice hojně, ale pouze určitým specializovaným způsobem. Stejně tak je možné říci, že čeští učitelé a učitelky se vyznačují výrazným smyslem pro morálku a slušnost. V konfrontaci s kriminální realitou mohou tyto vlastnosti vyznívat naivně. Učitelé musí být připravení, aby mohli působit preventivně, aby se orientovali v problematice bezpečnosti internetu a mohli být žákům dobrými rádci a oporou v krizových situacích.

V neposlední řadě je také potřeba zmínit, že v posledních letech narůstá počet virtuálních útoků na pedagogy. To znamená, že učitelé jsou čím dál častěji obětí internetové agrese. A to nejen její primitivní formy ze strany žáků, ale i propracovaných naříčení a šíření pomluv ze strany rodičů nebo dokonce kolegů. Jednoznačně lze říci, že dochází k nárůstu nebezpečí ohrožení učitelů. Je dobré vědět, které útoky nás ohrožují a jak se jim případně bránit.

2.2 Jak vypadá internetová kriminalita?

2.2.1 Spam

Spam je nepříjemná záležitost, se kterou se setkáváme v podstatě denně. Je to **nevyžádaná pošta**. Obecně lze za spam považovat i letáky supermarketů, nabídky na slevy a různé akce, které chodí do poštovních schránek.

V elektronické podobě se spam šíří pomocí **e-mailů**. Na první pohled nevypadají nijak nebezpečně, ale jejich škodlivost je opravdu vysoká. Nejméně si lidé uvědomují to, že spam je okrádá o čas. Prohlížení a mazání nevyžádané pošty, posuzování, zda se jedná o spam nebo nikoliv a odstraňování nevyžádané pošty, zabere většině lidí několik minut denně.

Dalším problémem je, že se spamem je možno někdy smazat i poštu důležitou. Stejně jako se nezřídka stává, že někdo spolu s letáky ze schránky vyhodí i složenky či dopis. Aby se lidé před spamem ochránili, instalují si antispamové programy. Což sice problém částečně řeší,

ale většinou to stojí peníze. Tyto záležitosti si obvykle jednotlivec neuvědomí, ale pro firmy disponující stovkami e-mailových účtů, se již jedná o velkou zátěž.

Největším problémem, který s sebou spam nese, je však často škodlivý obsah rozesílaných e-mailů. Zdaleka se tímto způsobem nešíří pouze neškodné reklamy. Velmi často e-mailový spam obsahuje i počítačové viry typu trojský kůň. Ty mohou v napadeném počítači pracovat jako rozesílač dalšího spamu. Takže napadený uživatel vůbec netuší, že z jeho počítače a někdy i jeho jménem, odchází škodlivá pošta. Škodlivost virů je všeobecně známa, proto je velmi důležité mít každý počítač vybavený antivirovým programem, u počítačů připojených k internetu je to naprostá nezbytnost.

2.2.2 Kyberšikana

Tento pojem je v současnosti bohužel velmi nadužíván a dochází i k matení představy o tom, co vlastně znamená. Často se pod pojem kyberšikana zahrnují i jiné jevy, které již mají v odborné literatuře své vlastní pojmenování.

Kyberšikana je opakované slovní **ubližování, napadání, ztrapňování, obtěžování či zastrašování** jiné osoby s využitím internetu, mobilního telefonu nebo jiných informačních technologií.

Projevem kyberšikany mohou být hanlivé, urážející nebo zesměšňující e-maily, SMS zprávy, příspěvky v diskuzi nebo chatu. Kyberšikana se může projevit také pořizováním zvukových záznamů, fotografií nebo videí, jejich následné (zesměšňující nebo urážející) úpravy, které mají za cíl poškodit zachycenou osobu. Dalším způsobem je vytváření webových stránek, které ponižují nebo jinak poškozují konkrétní osobu. Za kyberšikanu lze také považovat vytváření falešných osobních profilů na sociálních sítích nebo v diskuzích, kde se agresor vydává za svou oběť a diskredituje ji tím, že vystupuje jejím jménem takovým způsobem, za který se oběť může jenom stydět.

V poslední době se šíří nový způsob **kyberšikany učitelů**. Postup je takový, že jednotlivec nebo skupina žáků se snaží vyvést pedagoga z rovnováhy. Jde o různé drobné útoky při vyučování – házení papírků, klepání, vydávání zvuků, opakované nesmyslné žádosti, případně polohlasné poznámky a nadávky. V okamžiku, kdy učiteli ujedou nervy, je připraveno mnoho telefonů k natočení tohoto selhání. Podobných příspěvků se záznamem rozčileného pedagoga, je na internetu opravdu mnoho.

Velkým problémem je, že dohledat útočníka bývá velmi těžké a bez spolupráce s policií prakticky nemožné. Technologický postup vyhledání počítače, ze kterého byl nahrán konkrétní příspěvek na internet sice existuje, ale není vůbec jednoduchý a často nespolehlivý. Nehledě na to, že tyto nitky vedou většinou na nějaké veřejné místo jako je knihovna, internetová kavárna apod., kde se těžko zjišťuje, kdo v tu danou chvíli počítač použil.

Tip: Mnohem úspěšnější bývá tzv. personální šetření, tedy takové, kde se přímo ze znění urážlivých příspěvků dá posoudit, kdo je asi pachatelem.

Kyberšikana je věc, se kterou se ve svém okolí setkalo již 10 % žáků základních škol a 22 % studentů škol středních. Hanlivé příspěvky je většinou možné nějakým způsobem ze stránek odstranit, ale není to jednoduchá záležitost. Je nutno jednat se zřizovatelem konkrétních stránek a prokázat, že se jedná o škodlivý obsah.

Pokud někdo někoho urazí osobně, tak je to sice nepříjemné, ale jednak to za chvíli přebolí a za druhé se to dá také osobně řešit. Urážka vyvěšená na internetových stránkách je anonymní, útočník je neznámý a příspěvek tam zůstává po dlouhou dobu, po kterou je přístupný veřejnosti.

2.2.3 Kybergrooming

Jedná se o velmi nebezpečný jev, který může mít různé, ale vždy negativní až tragické důsledky. Kybergrooming je označení pro jednání osoby, která se snaží **zmanipulovat vyhlédnutou oběť** a donutit ji k osobní schůzce. Útočník s obětí komunikuje zejména prostřednictvím chatu, Skypu nebo SMS zpráv.

Cílem je vzbudit u oběti důvěru a získat důležité informace pro další manipulaci. Útočník se nejdříve snaží svou oběť izolovat od okolí větami typu:
Spolužáci, (kamarádi, rodiče) ti nerozumí, já jsem tvůj přítel, mě se můžeš svěřit…
Neříkej o tom ostatním dětem, žárlily by….
Neříkej o mě mamince, nenáviděla by tě….

Další komunikace má za cíl získat informace, které útočník potřebuje:
Máš počítač v pokojíčku, nebo v obýváku? Sleduje nás někdo?
Bydlíš v Praze? Já v Brně, budem přátelé na dálku? Později většinou útočník přidá výmysl, že náhodou jede do bydliště oběti. *Potkáme se?*
Máš mobil na kredit? Jaké máš zájmy? Útočník chce vědět, čím bude možné oběť případně v budoucnu uplácet.

Kybergroomingový útok končí zpravidla vylákáním oběti na osobní schůzku, kde dojde například k jejímu omámení, sexuálnímu zneužití, případně vraždě. Někdy je cílem útočníka únos oběti a požadování výkupného. Jsou známy i případy, kdy oběť vyzradí agresorovi dlouhodobou nepřítomnost rodiny v domácnosti, čehož on potom zneužije ke vloupání.

Odhalení kybergroomingu je velmi těžké, protože útočník je většinou dospělý a obětí dítě, které je manipulováno a poučováno útočníkem o tom, jak se neprozradit. Pro oběť má tato aktivita dlouho punc jakéhosi dobrodružství a zakázaného ovoce, což nahrává útočníkům. Cesty k odhalení vedou většinou přes pozorování chování dítěte-oběti. Vyhledávání soukromí při práci s počítačem, nevysvětlitelné částky zvyšující kredit mobilního telefonu, dárky přicházející poštou apod. Nutno dodat, že v dobře fungujících rodinách, kde rodiče s dětmi zdravě komunikují, nemají kybergroomingoví útočníci příliš šancí.

Při odhalení kybergroomingu je nutné přivolat policii a současně pokračovat opatrně v komunikaci „jménem oběti“, tak aby se útočník nevyplašil a na sjednané schůzce byl následně dopaden.

2.2.4 Kyberstalking

Nejdříve se podívejme na to, co se skrývá pod pojmem stalking. Jedná se velmi starý způsob obtěžování oběti. Je to **pronásledování**, opakované a stupňované obtěžování. Nejdříve například pomocí dopisů, vzkazů a následně opravdu fyzické stopování a pozorování oběti, případně její zastrašování. Jsou známy i případy, kdy cílem agresora nebylo oběť děsit, ale útočníkem byl člověk bezmezně zbožňující svou oběť.

Kyberstalking je zneužívání internetu, mobilních telefonů a dalších informačních technologií ke stalkingu. Je zřejmé, že takto provozovaný, nabývá stalking na intenzitě a často se stává veřejnou věcí. Obtěžování tohoto typu nemá většinou urážející nebo hanlivý podtext. Oběť trpí zejména ztrátou soukromí a pocitem pronásledování.

Výhodou pro odhalení stalkingu je to, že útočník často nechce zůstat v anonymitě. Sám svoji zvrácenou činnost chápe jako budování vztahu s obětí. Pro potření tohoto jednání je nutné, aby oběť shromažďovala důkazy a s nimi potom oslovila policii.

2.2.5 Hoax

Zdánlivě nejméně nebezpečným jevem v oblasti internetové kriminality je tzv. hoax. Jedná se ve své podstatě o **podvod**. Příčina i cíl hoaxu se může velmi lišit. Společným jevem všech hoaxů je jejich nepravdivost.

Anglické slovo hoax můžeme přeložit jako podvod, smyšlenka, výmysl, mystifikace. V přeneseném smyslu znamená novinářskou kachnu, poplašnou zprávu nebo kanadský žertík.

Hoax škodí různým způsobem, od nevinných a zábavných nesmyslů, až po velmi kruté a nebezpečné skutky, poškozující příjemce psychicky i finančně. Hoax se šíří pomocí spamu, ale mnohem častěji ho rozesílají sami uživatelé vědomě. Hoax někdy působí jako taková „šeptanda“ pomocí e-mailů. Určitě stojí za povšimnutí, že určité větvi hoaxu se velmi silně daří v postkomunistických evropských zemích a v oblastech s diktaturou. Jakoby zdejší uživatelé internetu stále věřili v existenci nějakých důležitých zatajovaných údajů.

Šíření hoaxu napomáhá nekritický příjem informací mnoha uživateli internetu. Hoaxové zprávy jsou často podávány jako seriózní oznámení, opřená o vědecká fakta, mezinárodní výzkumy nebo podvodné fotomontáže. A samozřejmě i fakt, že tyto zprávy často obdržíte od přátel nebo známých, tedy od těch, kteří již naletěli a hoax šíří v dobré víře, že pomáhají.

Příkladem neškodného hoaxu by mohl být článek, kde se tvrdí, že sloni se líhnou z vajec. Jejich kly jim slouží k vyklubání a chobotem vystrčeným ze skořápky v prvních okamžicích života dýchají. Škodlivý účinek bude, až na několik zmatených lidí slabších v biologii, prakticky nulový.

Mnohem horší jsou hoaxy vyvolávající paniku a strach. Jedná se třeba o zaručené zprávy o utajovaných únosech dětí do zemí třetího světa, nebo o přebalování neprodaného mléka, škodlivosti určitého typu zboží apod.

Jiné hoaxy zase nabízí nebezpečné rady. Příkladem jsou výzvy k vymazání, údajně škodlivých, souborů v počítači. Pokud čtenář poslechne, většinou si nevratně poškodí operační systém. Jiné hoaxy zase nabízejí zaručené léčebné metody na rakovinu, cukrovku, případně návody na zhubnutí, jejich uposlechnutí má většinou fatální následky.

Hoaxy, které lze opravdu kvalifikovat jako podvod s finanční újmou, jsou ty, které mají za cíl získání peněz na fingované účty. Tomuto druhu podvodu se říká *phishing* (jde o slovní hříčku, kterou lze přeložit jako *rybaření*). Většinou jsou doplněny výmluvnou fotografií trpícího člověka, která má vzbudit soucit, dále příběhem tohoto člověka se žádostí o finanční pomoc. Podvedený (ulovený) čtenář pak v dobré víře zasílá peníze podvodníkům. Obměn těchto e-mailů jsou desítky.

Tip: Jedinou smysluplnou ochranou proti hoaxu je zdravý úsudek, kritické myšlení a ověřování si informací z více zdrojů.

2.2.6 Happy slapping

Za opravdu zvrácenou zábavu lze považovat tzv. happy slapping, rozšířený zejména u teenagerů. Překlad tohoto pojmu znamená „šťastné fackování“. Základem je **natáčení útoku** agresora na nic netušící oběť. Jeden z útočníků pořizuje mobilním zařízením záznam a druhý, v roli toho „statečného“, napadá oběť. Pohlavkový útok je veden velmi často zezadu, na pisoáru, na sedícího apod. Tato videa jsou potom zveřejněna na internetu spolu s hlasováním, kde se hodnotí zejména rozčilená reakce napadené oběti.

Obzvlášť brutálními se tyto činy stávají, pokud jsou útoky vedeny proti bezmocným seniorům nebo spícím opilcům. Jsou známy i případy, kdy tyto útoky byly vedeny úderem pěstí a inzultovaná osoba potom upadla do bezvědomí. Za tyto útoky již byli pachatelé i odsouzeni.

Jiným druhem happy slappingu je *undress*. Jsou to opět natáčené útoky na nic netušící oběti. Těmi jsou v tomto případě mladá atraktivní děvčata, kterým útočník nečekaně strhne oblečení, většinou se jedná o letní šaty nebo trička bez ramínek. Tento nešvar se často realizuje na eskalátorech v obchodních domech, kde jsou děvčata natáčena s horních pater hned několika výrostky.

Všechny tyto útoky v sobě nesou vysokou společenskou nebezpečnost, dochází zde hned ke dvojímu ponížení. Jednak při samotném útoku a podruhé při vystavení natočených videí na internet. Pachatele se daří dopadnout většinou pouze v okamžiku vlastní natáčené výtržnosti, nebo těsně po ní. Naprostá většina však zůstává neodhalena.

2.2.7 Porušování autorských práv

Problémová činnost, která má za následek opravdovou finanční újmu nebo ušlý zisk fyzických osob i organizací. Jedná se v podstatě o krádeže uměleckých děl. V současné době je možné si na internetu neautorizovaně pustit mnoho filmů nebo neuvěřitelné množství hudebních klipů. A fotografie, které jsou stahovány, šířeny a využívány bez vědomí jejich autora, by nikdo nespočítal.

Sdílení, šíření a stahování souborů by se mělo dít vždy se souhlasem majitele autorských práv. V současnosti je autorský zákon v české republice nejčastěji porušovanou normou. Učitelé by měli dbát na to, aby na půdě školy nedocházelo k porušování zákonů.

2.2.8 Sexting

Rizikové sdílení a šíření materiálů sexuální povahy s použitím internetu či mobilních telefonů, je označováno jako sexting. Toto chování provozované mezi normálními sexuálními partnery by mohlo být chápáno jako neortodoxní zpestření vztahu. V současnosti však přibývá případů, kdy intimní fotky byly později zneužity, například po rozchodu nebo v průběhu partnerské krize. Držitel kompromitujícího materiálu může svou oběť vydírat, případně veřejně zostudit a ponížit.

Mnohem horším úkazem, se kterým je možné se čím dále častěji setkat, je výměna intimních fotografií nebo erotických materiálů mezi neznámými lidmi.

Je důležité, aby pedagog uměl rozumně a razantně zasáhnout v případě, že podobné chování u svých svěřenců odhalí.

2.2.9 Flaming, trolling

Pokud se někdo na internetu, zejména v diskuzích nebo na chatu, zbytečně rozohňuje, rozčiluje a nadává na cokoliv, aniž by přinášel a vyslechl (rozuměj: přečetl a komentoval)věcné a inteligentní argumenty, jedná se rizikový jev zvaný flaming. Jde o dehonestaci a bezdůvodné urážení osob, činností, neopodstatněnou kritiku autorských děl, napadání skupin obyvatelstva, menšin apod.

Trolling pak znamená, že se někdo chová neomaleně, vulgárně a sprostě. Internetovou diskuzi odvádí od tématu hloupými a nevhodnými poznámkami a narážkami. Místo toho, aby diskutoval, uráží diskutující. Jedná se o nestydatou exhibici lidí, kteří nedohlédnou účinku svých nevhodných, trapných a urážlivých slov.

Oba tyto jevy spolu úzce souvisí a často se prolínají. Dá se říci, že pramení z možnosti říkat anonymně, co kdo chce. Pokud někdo nemá co říci, říká sprosté hlouposti. Obzvlášť nebezpečné jsou tyto jevy v prostředí Facebooku mezi dětmi a mladistvými, protože mohou takové chování vzít za normu.

2.3 Jak na účinnou prevenci?

V boji s internetovou kriminalitou se jeví jako nejpodstatnější prvek prevence. Účinné předcházení naivnímu, hloupému, neslušnému a defektnímu chování je velmi důležité. Běžný uživatel internetu si většinou nebezpečí a ohrožení neuvědomuje. O nástrahách internetu se dozvídá jen útržkovitě a nesystematicky. Informovanost pedagogů je významnou složkou boje proti internetové kriminalitě.

2.3.1 Vliv rodiny

V současné době je běžné, že děti jsou mnohem zběhlejší v používání moderních technologií než jejich rodiče. Velmi jednoduše se jim může dařit zahlazovat stopy a důkazy o svém nevhodném chování na internetu.

Nejdůležitější je, aby v rodině panovala ohledně užívání internetu jasná pravidla. S jejich zavedením a prosazováním je potřeba začít hned, jakmile děti internet začnou užívat. Musí se stát samozřejmostí. Rodiče by měli prosazovat, aby k internetu za zábavou usedaly děti až po splnění ostatních povinností. Měla by být stanovena doba, jak dlouho a ve kterou denní dobu budou děti mít povoleno internet navštěvovat. Velmi důležité však je, aby si rodiče s dětmi o jejich zážitcích u počítače povídali, aby znali aktivity svých dětí a aby znali jejich případné virtuální přátele. Je potřeba budovat vztah založený na důvěře. V takové atmosféře se potenciální problémy dají úspěšně řešit.

Statistická data ukazují, že problémy s internetovou kriminalitou mají zejména děti a mladiství, kteří nemají pevné rodinné zázemí, nemají mnoho koníčků a nedokážou si organizovat svůj volný čas. Jednoznačně se potvrzuje, že tam, kde v rodině selhávají rodiče jako tvůrci pravidel a stavitelé mantinelů, dochází k mnohem častějším extrémním projevům a rizikovému chování.

2.3.2 Pomoc odborníků

Na internetu existují naštěstí stránky, které se věnují internetové kriminalitě, prevenci a bezpečnosti internetu. Každý zájemce zde může najít potřebné informace, cenné rady a hlavně účinné návody na to, jak se zachovat v případě ohrožení.

Mezi obsáhlé portály s obrovským množstvím informací, návodů, zpráv týkajících se této problematiky patří určitě projekt **E-bezpečí** (http://www.e-bezpeci.cz/index.php/home). Kromě popisu nebezpečných jevů, zde najdete i spoustu konkrétních kauz, zajímavých článků a návodů. Důležité je, že v rámci tohoto projektu probíhá i široké preventivní působení přímo na školách. Je možné pozvat si odborníky a nechat proškolit pedagogický sbor nebo přímo žáky.

Obrovským zdrojem informací je i web českého Centra bezpečnějšího internetu **SaferInternet.cz** (http://www.saferinternet.cz/). Zde najdete také odkazy na **Horkou linku** a **Linku bezpečí**. Tyto stránky by měly znát především děti, aby měly v případě potřeby možnost vyhledat odbornou pomoc. Na stránkách SaferInternet je také tlačítko určené k hlášení internetové kriminality. Centrum bezpečnějšího internetu provozuje také vynikající a užitečný portál **Bezpečně-online** (http://www.bezpecne-online.cz/uvod). Zde najdete mimo jiné i sekci *Poradna* nebo, stále více užívanější, část *Pro rodiče a učitele*.

Dalším dobrým zdrojem informací mohou být stránky **Hoax.cz**(http://www.hoax.cz/cze/), kam je dobré zajít tehdy, když obdržíte „zaručenou“ zprávu, kterou máte šířit dál. Ověření, zda se nejednalo o hoax, je většinou velmi rychlé. Dále stojí za zmínku obsažný portál **Viry.cz** (http://www.viry.cz/), kde se zájemci mohou dočíst nejen o virech, ale i o podvodných e-mailech a nejrůznějších způsobech napadání počítačů.

3 Škola a zákony

3.1 Školský zákon

Zákon 561/2004 Sb., který znáte pod názvem Školský zákon, je nejvyšším předpisem, kterým se musí školská zařízení v České republice řídit. Na nutnost vzdělávání s ohledem na bezpečnost a ochranu zdraví poukazuje hned paragraf 2, který se jmenuje Zásady a cíle vzdělávání, v jeho odstavci 2, písmeno „g", se říká: „*Získání a uplatňování znalostí o životním prostředí a jeho ochraně vycházející ze zásad trvale udržitelného rozvoje a o bezpečnosti a ochraně zdraví*."

Poznámka: V této kapitole se seznámíte se zněním některých právních předpisů. Pro lepší orientaci v textu budu uvádět stručný a přehledný zápis, ve kterém by citace v předešlém odstavci vypadala takto **§2,odst.2, písm. g)**: získání a uplatňování……..

Zákon nařizuje dodržování bezpečnosti i v mnoha dalších paragrafech. V dalším textu pokračuji jen těmi nejpodstatnějšími pro pedagogickou praxi.

Například **§22,odst. 1, písm. b)**žákům přímo nařizuje *dodržovat školní a vnitřní řád a předpisy a pokyny školy a školského zařízení k ochraně zdraví a bezpečnosti, s nimiž byli seznámeni*. Lze z něho tedy vyčíst povinnost nejen řády tvořit, ale žáky s nimi i seznamovat.

Bezpečnost a ochrana zdraví ve školách a školských zařízeních je uzákoněna v **§29,odst. 2** říká: *Školy a školská zařízení zajišťují bezpečnost a ochranu zdraví dětí, žáků a studentů při vzdělávání a s ním přímo souvisejících činnostech a při poskytování školských služeb a poskytují žákům a studentům nezbytné informace k zajištění bezpečnosti a ochrany zdraví. Ministerstvo stanoví vyhláškou opatření k zajištění bezpečnosti a ochrany zdraví dětí, žáků a studentů při vzdělávání ve školách a školských zařízeních a při činnostech s ním souvisejících.*

Velmi důležitý je celý paragraf **§ 30**o školním řádu:
(1) Ředitel školy vydá školní řád; ředitel školského zařízení vnitřní řád. Řád upravuje:
a) podrobnosti k výkonu práv a povinností dětí, žáků, studentů a jejich zákonných zástupců ve škole nebo školském zařízení a pravidla vzájemných vztahů s pedagogickými pracovníky,
b) provoz a vnitřní režim školy nebo školského zařízení,
c) podmínky zajištění bezpečnosti a ochrany zdraví dětí, žáků nebo studentů a jejich ochrany před sociálně patologickými jevy a před projevy diskriminace, nepřátelství nebo násilí,
d) podmínky zacházení s majetkem školy (školského zařízení) ze strany dětí, žáků a studentů.
(2) Školní řád obsahuje také pravidla pro hodnocení výsledků vzdělávání žáků a studentů.
(3) Školní řád nebo vnitřní řád zveřejní ředitel na přístupném místě ve škole nebo školském zařízení, prokazatelným způsobem s ním seznámí zaměstnance, žáky a studenty školy nebo školského zařízení a informuje o jeho vydání a obsahu zákonné zástupce nezletilých dětí a žáků.

Z výše napsaného vyplývá, že škola jako instituce musí dbát na bezpečnost žáků, svých zaměstnanců i svého majetku. Školní řád, který vydává, je závazný pro všechny účastníky vyučovacího procesu. K tématu této příručky je nutné říci, že školní řád je potřeba rozšířit o vnitřním směrnice, které zajišťují pravidla v odborných učebnách. Učebny výpočetní techniky a informatiky nejsou výjimkou.

3.2 Autorský zákon

Zákon 121/2000 Sb. nese název **Zákon o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů**.

Tento zákon stanovuje, co lze považovat za autorské dílo a co nikoliv. Zejména však vymezuje pravidla nakládání s autorskými díly, kdy je možné do díla zasahovat, upravovat jej a nakládat s ním. Pro pedagogickou práci je důležité ustanovení **§ 31,odst. 1, písm. c).** Celý první odstavec zní takto:
(1) Do práva autorského nezasahuje ten, kdo
a) užije v odůvodněné míře výňatky ze zveřejněných děl jiných autorů ve svém díle,
b) užije výňatky z díla nebo drobná celá díla pro účely kritiky nebo recenze vztahující se k takovému dílu, vědecké či odborné tvorby a takové užití bude v souladu s poctivými zvyklostmi a v rozsahu vyžadovaném konkrétním účelem,
c) užije dílo při vyučování pro ilustrační účel nebo při vědeckém výzkumu, jejichž účelem není dosažení přímého nebo nepřímého hospodářského nebo obchodního prospěchu, a nepřesáhne rozsah odpovídající sledovanému účelu;
vždy je však nutno uvést, je-li to možné, jméno autora, nejde-li o dílo anonymní, nebo jméno osoby, pod jejímž jménem se dílo uvádí na veřejnost, a dále název díla a pramen.

Dále**§ 35,odst. 2** říká: *Do práva autorského nezasahuje ten, kdo nikoli za účelem přímého nebo nepřímého hospodářského nebo obchodního prospěchu užije dílo při školních představeních, v nichž účinkují výlučně žáci, studenti nebo učitelé školy nebo školského či vzdělávacího zařízení.*

A také v**§ 35,odst. 3** se praví: *Do práva autorského také nezasahuje škola nebo školské či vzdělávací zařízení, užije-li nikoli za účelem přímého nebo nepřímého hospodářského nebo obchodního prospěchu k výuce nebo k vlastní vnitřní potřebě dílo vytvořené žákem nebo studentem ke splnění školních nebo studijních povinností vyplývajících z jeho právního vztahu ke škole nebo školskému či vzdělávacímu zařízení (školní dílo).*

Kopírování a rozmnožování autorských děl řeší **§ 30a,odst. 1:**

Rozmnožování na papír nebo na podobný podklad
(1) Do práva autorského nezasahuje
a) fyzická osoba, která pro svou osobní potřebu,
b) právnická osoba nebo podnikající fyzická osoba, která pro svou vlastní vnitřní potřebu,
c) ten, kdo na objednávku pro osobní potřebu fyzické osoby,
d) ten, kdo na objednávku pro vlastní vnitřní potřebu právnické osoby nebo podnikající fyzické osoby zhotoví tiskovou rozmnoženinu díla na papír nebo podobný podklad fotografickou technikou nebo jiným postupem s podobnými účinky, s výjimkou případu, kdy jde o vydaný notový záznam díla hudebního či hudebně dramatického, a v případech podle písmen

Všeobecně lze říci, že pokud pedagog nakládá s autorským dílem pro potřebu výuky, potažmo školy a nevyplývá z toho pro něj další finanční zisk, nijak se proti autorskému právu neproviňuje. V okamžiku, kdy použití autorského díla generuje osobě zisk, je situace problematická.

3.3 Zákon BOZP

Zákon o zajištění dalších podmínek bezpečnosti a ochrany zdraví při práci (BOZP) nese číslo 309/2006 Sb. Upravují se jím požadavky bezpečnosti a ochrany zdraví při práci v pracovněprávních vztazích a o zajištění bezpečnosti a ochrany zdraví při činnosti nebo poskytování služeb mimo pracovněprávní vztahy.

Ve školství je nejdůležitější část (**§9**), která stanoví povinnosti zaměstnavatele, tedy školy zastoupené ředitelem jako statutárním orgánem.

(1) Zaměstnavatel je povinen zajišťovat a provádět úkoly v hodnocení a prevenci rizik možného ohrožení života nebo zdraví zaměstnance (dále jen "zajišťování úkolů v prevenci rizik") s ohledem na

a) nebezpečí ohrožení bezpečnosti a zdraví zaměstnanců při práci ve vztahu k předmětu činnosti zaměstnavatele,

b) základní znalosti a dovednosti zaměstnanců,

c) počet zaměstnanců, jejich odbornou připravenost a jimi vykonávanou práci.

(2) Zaměstnavatel může zajišťovat plnění úkolů v prevenci rizik, je-li k tomu způsobilý nebo odborně způsobilý v případech a za podmínek uvedených v odstavci 3 písm. a) a b) sám, jinak je povinen zajistit tyto úkoly odborně způsobilým zaměstnancem, kterého zaměstnává v pracovněprávním vztahu 6). Nemá-li takového zaměstnance, je povinen zajistit je jinou odborně způsobilou osobou. Odborně způsobilý zaměstnanec zaměstnavatele nebo jiná odborně způsobilá fyzická osoba jsou odborně způsobilými osobami.

(3) Zaměstnává-li zaměstnavatel

a) nejvýše 25 zaměstnanců, může zajišťovat úkoly v prevenci rizik sám, má-li k tomu potřebné znalosti,

b) 26 až 500 zaměstnanců, může zajišťovat úkoly v prevenci rizik sám, je-li k tomu odborně způsobilý, nebo jednou nebo více odborně způsobilými osobami,

c) více než 500 zaměstnanců, zajišťuje úkoly v prevenci rizik vždy jednou nebo více odborně způsobilými osobami.

(4) Zaměstnavatel je povinen

a) poskytnout odborně způsobilé osobě k zajišťování úkolů v prevenci rizik zejména potřebné prostředky a dobu potřebnou k výkonu její činnosti, zvláště ve vztahu k zaměstnancům v pracovním poměru na dobu určitou 7), mladistvým zaměstnancům 8), těhotným zaměstnankyním, zaměstnankyním, které kojí, nebo zaměstnankyním - matkám dítěte do konce devátého měsíce po porodu a zaměstnancům agentury práce 9) dočasně přiděleným k výkonu práce k jinému zaměstnavateli,

b) zajistit dostatečný počet odborně způsobilých osob,

c) poskytnout odborně způsobilé osobě dokumentaci a informace

1. o všech skutečnostech a okolnostech, o nichž je mu známo, že mají nebo by mohly mít vliv na bezpečnost zaměstnanců nebo vést k poškození jejich zdraví,

2. podané zaměstnancům jiného zaměstnavatele, které obdrželi před zahájením práce na pracovištích zaměstnavatele k zajištění bezpečnosti a ochrany zdraví při práci.

(5) Při zajišťování úkolů v prevenci rizik postupuje odborně způsobilá osoba v součinnosti s odborně způsobilými fyzickými osobami vykonávajícími svoji působnost podle zvláštních právních předpisů 10), s odborovou organizací a zástupcem pro oblast bezpečnosti a ochrany zdraví při práci 11).

Důležité je, že každý zaměstnavatel musí vyhodnocovat a snažit se preventivně odstraňovat veškerá rizika. Ohrožení internetovou kriminalitou však zatím nejsou na českých školách příliš zohledňována. Metodik ICT na školách by měl být prvním, kdo na podobná rizika upozorní a bude usilovat o jejich nápravu.

3.4 Vyhlášky MŠMT, vnitřní směrnice a řády učeben

Dalším nižším stupněm předpisů jsou vyhlášky a metodické pokyny Ministerstva školství, mládeže a tělovýchovy. Nejvýznamnější je vyhláška 48/2005 Sb. MŠMT ze dne 18. ledna 2005 o základním vzdělávání a některých náležitostech plnění povinné školní docházky.

V této vyhlášce zdůrazňuje povinnost školy dbát o bezpečnost svých žáků **§ 3,odst. 1**:*Bezpečnost a ochranu zdraví žáků ve škole, při vzdělávání mimo místo, kde se uskutečňuje vzdělávání 1), a při akcích konaných mimo místo, kde se uskutečňuje vzdělávání, zajišťuje právnická osoba, která vykonává činnost školy, svými zaměstnanci, vždy však nejméně jedním pedagogickým pracovníkem 2). Zaměstnance, který není pedagogickým pracovníkem, může ředitel školy k zajištění bezpečnosti a ochrany zdraví žáků určit pouze, pokud je zletilý a způsobilý k právním úkonům*.

Nepravidelně vycházejícími koncepčními předpisy a doporučeními, které vydává MŠMT, jsou tzv. **metodické pokyny**. Tématu této příručky se podrobně věnuje zejména Metodický pokyn č. 22294/2013-1Ministerstva školství, mládeže a tělovýchovy k řešení šikanování ve školách a školských zařízeních. Zde je v **Čl. 1, odst. 2** popsána kyberšikana takto: *Kyberšikana je jednou z forem psychické šikany. Je to zneužití ICT (informačních a komunikačních technologií), zejména pak mobilních telefonů a internetu, k takovým činnostem, které mají někoho záměrně ohrozit, ublížit mu. Podobně jako u šikany tváří v tvář se jedná o úmyslné chování, kdy je oběť napadána útočníkem nebo útočníky. Povaha a provedení útoků pak určuje její závažnost.*

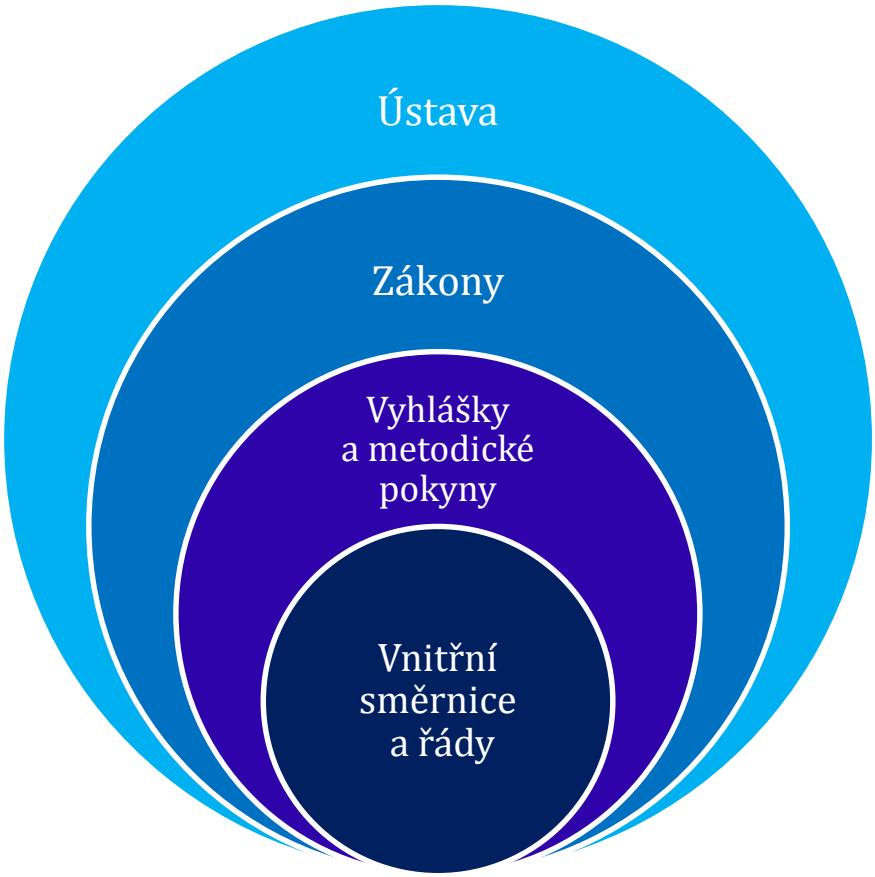
V odstavci **5, písm. a),b)** se říká: *a) Kyberšikanou není oprávněná kritika na internetu bez zlého úmyslu, bez nadávek a ponižování. Termínem kyberšikana neoznačujeme rovněž vzájemné internetové psychické násilí a ani věcný konflikt (i opakovaný) mezi rovnocennými partnery.*

b) Od kyberšikany je potřeba odlišovat příbuzné fenomény, které jsou často s kyberšikanou provázány nebo se s ní částečně překrývají, nicméně samy o sobě označují jiný typ násilného chování. Patří mezi ně například happy slapping, sexting, hoax, spam, cyberstalking, flaming, phising.

Minimální požadavky na školu pro řešení šikany řeší **Čl. 5** konkrétními nařízeními, která musí obsahovat školní řád: *kategorický zákaz chování mající charakter šikanování a opatření, která se váží k tomuto závažnému porušení školního řádu, zpracovaná pravidla používání informačních a komunikačních technologií, internetu a mobilních telefonů (během vyučování, o přestávkách, v prostoru školy). Součástí tohoto textu je i stanovení kázeňských opatření při nedodržování těchto pravidel.*

Dalším metodickým pokynem, který se zabývá využíváním internetu ve školách je **metodický pokyn č. 30799/2005-55**, jenž stanovuje standard ICT služeb ve škole a náležitosti dokumentu „ICT plán školy". Zde se řeší zejména bezpečnost osobních údajů, nutnost zálohování dat, nutnost stanovit bezpečnostní pravidla pro využívání ICT technologií a právní důsledky nedodržení bezpečnostních předpisů.

Na základě zákona 561/2004 Sb., vydává ředitel školy, jako statutární orgán **Školní řád, vnitřní směrnice a řády odborných učeben.** Všechny tyto předpisy jsou závazné pro všechny účastníky vyučovacího procesu. V poslední době existuje dobře znatelný a jednoznačně správný trend, zanášet do vnitřních školních předpisů i preventivní opatření proti internetové kriminalitě a pravidla zamezující zneužití ICT technologií ve školách.



4 Řády odborných učeben

4.1 Jak má vypadat řád odborné učebny?

Protože se zde zabýváme problematikou internetu, bude se další text věnovat zejména řádům v učebnách informatiky a výpočetní techniky.

Oproti předpisům zmíněných v předešlých kapitolách, má být řád odborné učebny velice konkrétní, přesný a jednoznačný. Jedná se o vnitřní předpis, který má zajistit bezpečnost a správné chování v dané učebně. Není to všeobecný popis správného chování. Může být až adresný, s popisem jednotlivého vybavení učebny, výčtem oprávněných osob, může zahrnovat kontakty na tyto osoby, časové údaje (od kdy do kdy je něco možné), apod.

Řád odborné učebny by měl v učebně být viditelně vyvěšen a přístupný kdykoliv, všem návštěvníkům učebny.

Řád učebny informatiky by měl jednoznačně definovat způsob a pravidla při užívání veškerého zařízení. Měl by obsahovat souhrnná pravidla pro práci s počítači a jejich příslušenstvím. Dále by mělo být jednoznačně stanoveno, kdy a za jakých podmínek je možné používat společná zařízení, jako je například interaktivní tabule s dataprojektorem, síťová tiskárna, skener, plotter apod. Tento řád by měl přesně vymezovat pravidla pro používání wifi, včetně toho, kdy a zda vůbec se mohou připojovat žáci, případně cizí návštěvníci školy.

4.1.1 Náležitosti řádu odborné učebny

Platný řád odborné učebny by měl být vždy formulován stručně a jasně, nejlépe v bodech. Každý řád by měl obsahovat následující formální náležitosti:

- název školy, která řád vydává
- název odborné učebny, popř. číslo dveří
- titul, jméno a příjmení ředitele školy
- podpis ředitele školy
- datum vydání řádu
- hranaté razítko školy

4.2 Praktické příklady

4.2.1 Co by v řádu odborné učebny informatiky nemělo chybět?

Podívejme se na základní nástin bodů, na které bychom při psaní řádu odborné učebny informatiky a výpočetní techniky neměli zapomenout:

1) Do učebny vstupují žáci jen s doprovodem vyučujícího.

2) Každý žák se před zapnutím počítače zapíše do provozního deníku, který je u každého počítače – své jméno, třídu, datum a dobu, po kterou na počítači bude pracovat, ev. všechny závady, které na svém počítači nebo pracovišti zjistí. Závady musí nahlásit vyučujícímu.

3) Žák pracuje u počítače podle pokynů vyučujícího, manipuluje s počítačem a jeho periferiemi pouze způsobem, se kterým byl seznámen učitelem v rámci výuky.

4)V učebně žáci nejedí a nepijí, aby nepoškodili vybavení učebny, například znečištěním klávesnice. Žáci musí mít při práci čisté ruce a dbát na hygienu při práci s počítačem.

5) Žáci bez svolení vyučujícího nepracují na řídícím počítači, nemanipulují s připojením počítačů k napájecímu zdroji, počítačové síti a k periferiím.

6) Žáci nepřinášejí do učebny vlastní CD, DVD nebo flashdisky apod. s programy a nesnaží se je používat. Nekopírují programy z počítače pro své potřeby, protože by tím porušili autorská práva, dopustili se tak trestného činu a vystavili se nebezpečí trestního stíhání.

7) Jakékoliv neobvyklé chování počítače ohlásí neprodleně žáci učiteli.

8) Žáci při práci s počítačem neprovádějí žádné operace, které by mohly ohrozit nastavení konfigurace počítače, poškodit nebo zničit software a hardware, protože by mohli způsobit poruchu počítačů a značnou finanční škodu. Při práci s interaktivní tabulí se žáci řídí výhradně pokyny vyučujícího. Je zakázáno psát na interaktivní tabuli čímkoliv jiným, než jsou elektronické tužky (příslušenství tabule).

9) Žáci využívají internet pouze pro potřeby výuky a s výslovným svolením vyučujícího. Stahování jakýchkoliv materiálů je možné pouze se svolením vyučujícího. Uživatelům jsou zakázány jakékoliv instalace programů. Požadavky na instalaci programů hlaste správci učebny.

10) Pokud žáci svévolným porušením tohoto řádu způsobí škodu na vybavení učebny, bude od nich vymáhána finanční náhrada – koupě nového vybavení, programů, úhrada práce opraváře, apod. Žáci jsou proto na začátku školního roku seznámeni i se současnými cenovými relacemi výpočetní techniky.

11) Uživatelé ukládají svou práci výhradně do určených složek (Dokumenty…). Nemění nastavení Plochy.

12) Žáci se v učebně chovají tak, aby neohrozili zdraví svoje, ani ostatních osob v učebně. S vybavením učebny zacházejí šetrně. Počítače se vypínají pouze na pokyn vyučujícího, je nutné vypnout i monitor. Počítače se vypínají poslední vyučovací hodinu každého dne.

13) Vzhledem k vysoké ceně vybavení učebny bude porušení tohoto řádu považováno za velmi závažný kázeňský přestupek.

14) Správcem učebny je: XY, kontakt.

Tip: Řád odborné učebny může být samozřejmě i mnohem stručnější, heslovitý a tím možná lépe zapamatovatelný a vymáhatelný. Stručné pojetí řádu potom vyznívá mnohem direktivněji a důrazněji:

1) Nevstupuj bez dozoru.

2) Před prací zkontroluj počítač.

3) Nejez, nepij, buď čistotný.

4) Závady a poruchy hlas vyučujícímu.

5) Nic nestahuj, neinstaluj.

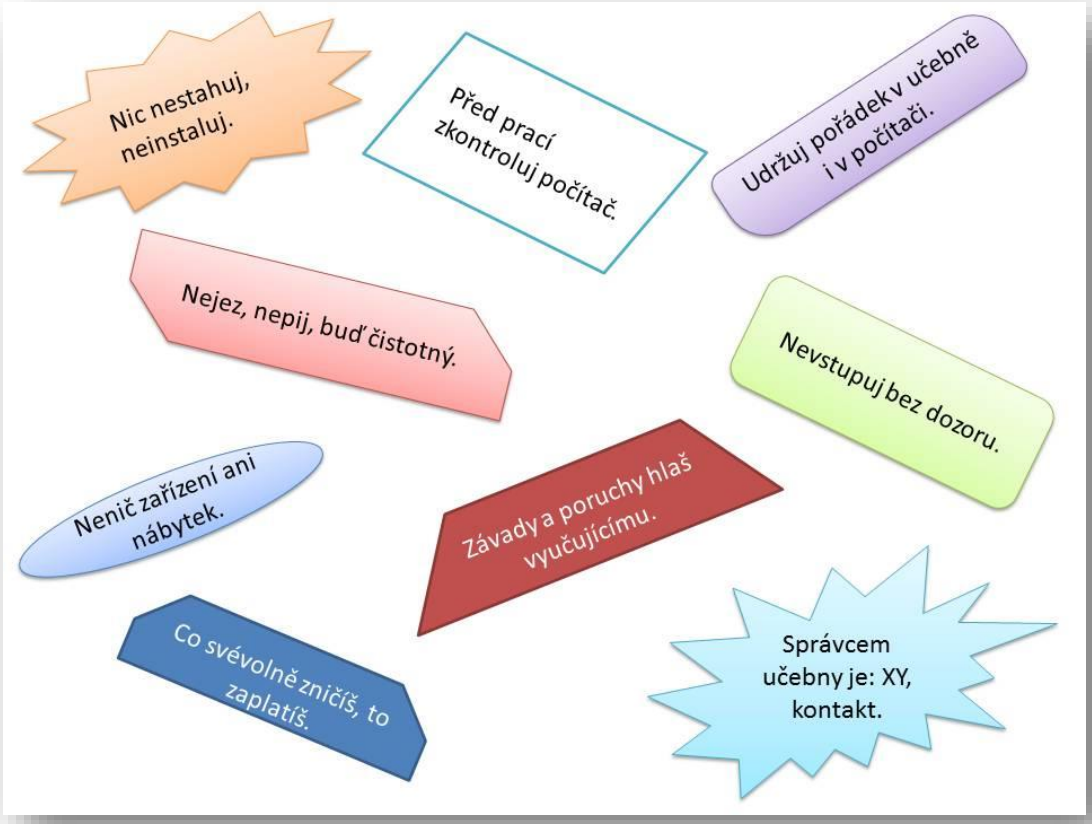
6) Nenič zařízení ani nábytek.

7) Udržuj pořádek v učebně i v počítači.

8) Co svévolně zničíš, to zaplatíš.

9) Správcem učebny je: XY, kontakt.

Takto pojatý řád odborné učebny je potom možno „změkčit“ konkrétním pojetím jeho provedení. Velmi dobře se osvědčuje nástěnka, kde jsou jednotlivé pokyny graficky různě ztvárněny, tak aby byly srozumitelné a žákům stále na očích.



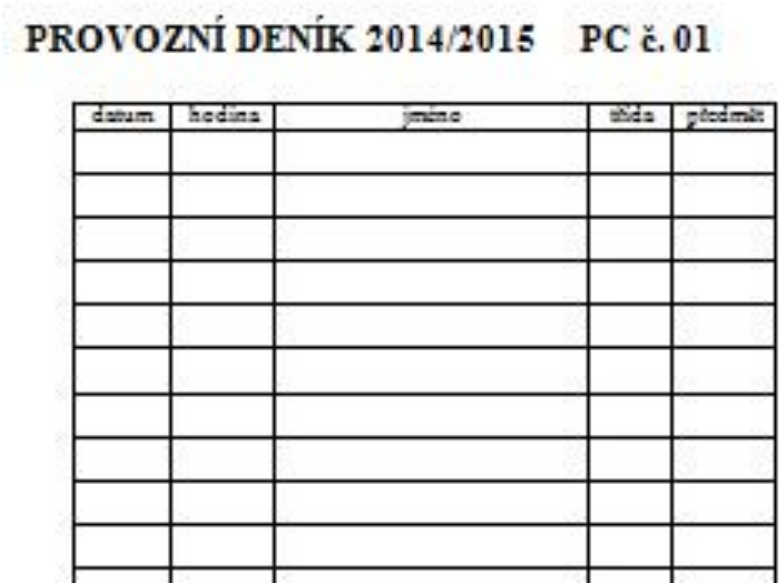
Tip: Pokud chceme, aby žáci pravidla v odborné učebně vnímali a řídili se jimi, je dobré, aby se spolupodíleli na jejich tvorbě. V rámci některých úvodních hodin na začátku školního roku je možné pojmout vytvoření námětu na podobnou nástěnku jako soutěž v rámci třídy, případně mezi třídami.

Žáci mnohdy přijdou na mnohá kreativní řešení, kterými mohou nejen vyzdobit učebnu, ale která jim zejména umožní to, aby vzali řád odborné učebny za svůj.

Na závěr je nutno říci, že v žádném případě není dobré podceňovat rizika spojená s používáním ICT technologií. Počítačová a internetová kriminalita je na vzestupu a je povinností školy a pedagogů své svěřence před ní chránit. Jedná se o povinnost nejen morální, ale i zákonem stanovenou.

4.3 Provozní deník

Vhodným opatřením, které se osvědčuje v praxi, je zavedení tzv. Provozního deníku. V podstatě stačí pouze dvojlist papíru, který bude neustále k dispozici u každého počítače. Žák, který přijde do učebny, se nejdříve do deníku musí zapsat. V deníku je dobré požadovat zápis jména, třídy, vyučovací hodiny a předmětu, ve kterém je žák u počítače.

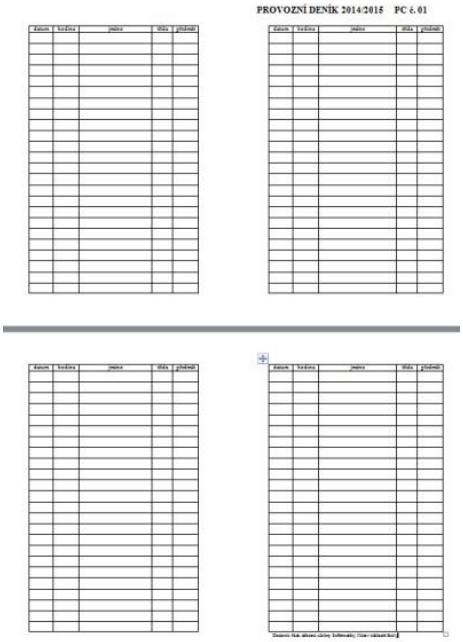


PROVOZNÍ DENÍK 2014/2015 PC č. 01

datum	hodina	jméno	třída	předmět

Provozní deník může dobře posloužit jednak k dohledání viníků poškození zařízení, ale zejména má silný preventivní charakter. Zbavuje uživatele anonymity, a tak jej nutí chovat se správně a ctít pravidla a řád odborné učebny.

Velice dobře se osvědčuje uspořádání čtyř těchto tabulek na dvě stránky jednoho listu. Pokud tento dokument vytisknete oboustranně a přeložíte, získáte deník k jednomu počítači na několik měsíců.



5 Použité zdroje

[1] http://www.e-bezpeci.cz/index.php/home

[2] http://www.saferinternet.cz/

[3] http://www.bezpecne-online.cz/uvod

[4] http://www.hoax.cz/cze/

[5] http://www.viry.cz/

[6] http://www.vetsonmedia.com/wp-content/uploads/2014/07/troll-2.jpg

[7] 121/2000 Sb. ZÁKON ze dne 7. dubna 2000 o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění zákonů č. 81/2005 Sb., č. 61/2006 Sb., č. 186/2006 Sb., č. 216/2006 Sb., č. 168/2008 Sb., č. 41/2009 Sb., č. 227/2009 Sb., č. 153/2010 Sb., č. 424/2010 Sb., č. 375/2011 Sb., č. 420/2011 Sb., č. 18/2012 Sb., č. 496/2012 Sb., č. 156/2013 Sb., č. 303/2013 Sb. a č. 64/2014 Sb.

[8] 561/2004 Sb.ZÁKON ze dne 24. září 2004o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon)ve znění zákonů č. 383/2005 Sb., č. 112/2006 Sb., č. 158/2006 Sb., č. 161/2006 Sb., č. 165/2006 Sb., č. 179/2006 Sb., č. 342/2006 Sb., č. 624/2006 Sb., č. 217/2007 Sb., č. 296/2007 Sb., č. 343/2007 Sb., č. 58/2008 Sb., č. 126/2008 Sb., č. 189/2008 Sb., č. 242/2008 Sb., č. 243/2008 Sb., č. 306/2008 Sb., č. 384/2008 Sb., č. 49/2009 Sb., č. 227/2009 Sb., č. 378/2009 Sb., č. 427/2010 Sb., č. 73/2011 Sb., č. 331/2011 Sb., č. 375/2011 Sb., č. 420/2011 Sb., č. 472/2011 Sb., č. 53/2012 Sb., č. 333/2012 Sb., č. 370/2012 Sb., č. 241/2013 Sb., zákonného opatření č. 344/2013 Sb. a zákona č. 64/2014 Sb.

[9] 309/2006 Sb.ZÁKON ze dne 23. května 2006, kterým se upravují další požadavky bezpečnosti a ochrany zdraví při práci v pracovněprávních vztazích a o zajištění bezpečnosti a ochrany zdraví při činnosti nebo poskytování služeb mimo pracovněprávní vztahy (zákon o zajištění dalších podmínek bezpečnosti a ochrany zdraví při práci)ve znění zákonů č. 362/2007 Sb., č. 189/2008 Sb., č. 223/2009 Sb., č. 365/2011 Sb., č. 375/2011 Sb. a č. 225/2012 Sb.

[10] 48/2005 Sb.VYHLÁŠKA Ministerstva školství, mládeže a tělovýchovy ze dne 18. ledna 2005 o základním vzdělávání a některých náležitostech plnění povinné školní docházky ve znění vyhlášek č. 454/2006 Sb. a č. 256/2012 Sb.

[11] Metodický pokyn Ministerstva školství, mládeže a tělovýchovy č. 22294/2013-1, k řešení šikanování ve školách a školských zařízeních

[12] Metodický pokyn Ministerstva školství, mládeže a tělovýchovy č. 30799/2005-551, stanovující „Standard ICT služeb ve škole“ a náležitosti dokumentu „ICT plán školy“ jako podmínky čerpání účelově určených finančních prostředků státního rozpočtu.