

Zásady využívání ICT

na ZŠ Planá nad Lužnicí

Tyto zásady jsou platné pro všechny zaměstnance a studenty, zástupce externích subjektů a třetích stran, kteří spolupracují se školou. Cílem těchto zásad je přijetí veškerých možných a nezbytných opatření k ochraně dat a informačních systémů školy před zavirováním, neoprávněným přístupem, poškozením, ztrátou, zneužitím či krádeží. Školní počítačový systém bude všemi uživateli využíván profesionálně, legálně a eticky.

Základní ustanovení	1
Práva a povinnosti uživatelů ICT	1
Přístupová práva uživatelů k informačním systémům	2
Povinnosti uživatelů informačních systémů	2
Povinnosti uživatelů informačních systémů při bezpečnostním incidentu	3
Datová síť	3
Připojení koncových zařízení do sítě	3
Uživatelská koncová zařízení	3
Koncová serverová zařízení	4

1. Základní ustanovení

Informační systémy a ICT zahrnují zejména, nikoliv však výlučně, sítě, data a jejich úložiště, online a offline komunikační technologie a zařízení pro přístup k nim, např.: mobilní telefony, tablety, digitální fotoaparáty, email a stránky na sociálních sítích. ICT může být využíváno pouze oprávněnými uživateli, a to jen pro plnění studijních, organizačních a pracovních úkolů, které plynou z pracovněprávního nebo studijního poměru. Uživatelé soukromých zařízení připojených do počítačové sítě či jinak využívající ICT školy jsou povinni dodržovat pravidla platná pro počítačové sítě stejně tak jako všechny platné legislativní předpisy. Školní informační systém musí být užíván tak, aby neporušoval zákon 40/2009 Sb. (trestní zákoník), který definuje podstatu trestných činů (získání materiálu s úmyslem spáchat nebo usnadnit páčání trestného činu, úprava počítačového materiálu bez povolení a podobně). Na ICT smí být používán pouze legálně získaný software, a to jen za dodržování příslušných licenčních podmínek a doby platnosti tohoto softwaru. Je zakázáno neoprávněné šíření nebo používání programu a dat, které jsou v rozporu s licenčními nebo jinými pravidly, totéž platí i pro zkušební používání softwaru (shareware, trial). Správu ICT a celého informačního systému zajišťují pověřené osoby. Tyto pověřené osoby jsou oprávněny k monitorování provozu zařízení připojených k síti. V případě zjištění porušování pravidel ze strany uživatele jsou povinni tomuto porušování zabránit. Pověřená osoba je při monitorování provozu povinna dodržovat všechna legislativní nařízení, která se na danou oblast vztahují, včetně předpisů pro ochranu osobních dat. Chci-li zabránit neoprávněnému přístupu k systému nebo k osobním údajům, nebudu nechávat tento informační systém bez odhlášení se ze systému nebo náležitého uzamčení přístupu heslem.

2. Práva a povinnosti uživatelů ICT

Uživatelé ICT jsou povinni dodržovat následující pravidla: hromadné e-mailové zprávy lze v nezbytném rozsahu rozesílat pouze za účelem plnění pracovních povinností, a to jen okruhu příjemců, kterým daná zpráva náleží. Uživatel nesmí používat jakékoli neoprávněné získané licenční klíče, kódy a hesla či jiné prostředky sloužící k obcházení zajištění informační bezpečnosti a ochrany počítačových programů. Uživateli je zakázáno odstranit jakékoliv informace, označení či zařízení identifikující nositele či vykonavatele autorských práv k počítačovým programům a datům podléhajícím autorskému zákonu. Uživatel je povinen umožnit kontrolu zařízení vykonávanou pověřenou osobou. Nesmí vytvářet nebo pozměňovat data s cílem ovlivnit kontrolu oprávněnosti užití počítačových programů. Není povoleno jakkoli bránit v kontrole vybavení ICT.

Informační systém pro elektronickou poštu, přístup k informačnímu systému nebo internetu (včetně sociálních sítí) musí být využíván v souladu s platnými normami. Nesmí být zneužit proti zájmům školy, ani k používání k soukromým podnikatelským aktivitám zaměstnanců a žáků. Dále je zakázáno využívat elektronické pošty k šíření jakýkoliv pomlouvačných, urážlivých, obscénních či výhružných materiálu, k šíření násilí, rasismu, nesnášenlivosti, xenofobie, pornografie, k propagaci politických názorů, hnutí a skupin směřujících k potlačení práv a svobod občanů a k šíření reklamních zpráv.

3. Přístupová práva uživatelů k informačním systémům

Každý uživatel se hlásí k informačním systémům na základě svého uživatelského účtu, který je chráněn uživatelským jménem a heslem. Daný účet má přiřazeny předdefinované sady oprávnění dle pracovní náplně uživatele nebo potřeb pro výuku. Každý uživatel, který chce užívat služeb informačních systémů musí být registrován a musí být známa jeho identita (totožnost osoby). Přístup uživatele k počítačové síti musí být vždy chráněn dostatečně silným heslem.

4. Povinnosti uživatelů informačních systémů

Uživatel se při tvorbě hesla řídí pravidly, která zajišťují používání kvalitních hesel:

- nesdělovat další osobě
- heslo musí být dostatečně silné, aby se nedalo jednoduše strojově nebo ručně prolomit (ideálně kombinace malých a velkých písmen a číslic, délka alespoň 6 znaků)
- mělo by být pravidelně měněno v závislosti na rizicích spojených s prolomením
- hesla se musí změnit v případě jakéhokoli náznaku možného kompromitování systému nebo hesla
- uživatel nese odpovědnost za prozrazení jeho hesla a následné zneužití svého účtu

Uživatelé jsou povinni zajistit bezpečnost uživatelských zařízení, a to zejména pracovních stanic, kdy se v případě ukončení nebo přerušení práce a odchodu z pracoviště musí odhlásit, případně zamknout pracovní stanici. Žáci jsou povinni po ukončení výuky v učebně odhlásit nebo vypnout pracovní stanici. Pokud uživatel záměrně nebo svou nedbalostí umožní využívání ICT jiné osobě, je plně zodpovědný za následky a škody s tím vzniklé. Uživatel nesmí záměrně nebo bez závažného důvodu přetěžovat počítačovou síť nebo se snažit získat neoprávněný přístup k informacím, datům nebo přístupovým údajům jiných účastníků. Pokud uživatel zjistí, že přístup k takovým údajům má, je povinen tuto skutečnost neprodleně oznámit pověřené osobě pro správu informačních systémů.

5. Povinnosti uživatelů informačních systémů při bezpečnostním incidentu

Bezpečnostní incident je definován jako porušení bezpečnosti systému, kdy je v rozporu s bezpečnostní politikou získán přístup k informacím nebo zdrojům systému. V případě důvodného podezření na vznik bezpečnostního incidentu přeruší koncový uživatel neprodleně práci a informuje pověřenou osobu nebo vedoucího zaměstnance.

6. Datová síť

Provozní pravidla datové sítě, veškerá nastavení nebo instalaci kabeláže či zařízení v síti může provádět pouze pověřená osoba. Pověřená osoba vede patřičnou dokumentaci o typologii zařízení a nastavení těchto zařízení v síti. Pověřená osoba může odpojit taková zařízení, která negativně ovlivňují chod ostatních zařízení nebo jejichž provoz je v rozporu s těmito pravidly. Pověřená osoba neprodleně informuje o odpojení daného uživatele odpovědného za chod zařízení.

7. Připojení koncových zařízení do sítě

Instalaci koncového zařízení, které je v majetku školy, a jeho připojení do počítačové sítě provádí pověřená osoba. Každé zařízení připojené do počítačové sítě musí splňovat požadavky pro bezproblémový provoz. Není povoleno zařízení nebo jeho části přemísťovat bez vědomí pověřené osoby, pokud k tomu nejsou závažné důvody (ohrožení života, zdraví či majetku). Uživatel je povinen udržovat zařízení způsobem daným výrobcem nebo pověřenou osobou, předcházet možnému poškození, zničení a ztrátě. Veškeré nákupy koncových zařízení musí být předem schváleny pověřenou osobou. Při nákupu koncových zařízení musí pověřená osoba zajistit kompatibilitu se stávající hardwarovou a softwarovou strukturou.

8. Uživatelská koncová zařízení

Každé koncové zařízení má určenou osobu (správce), která odpovídá za provoz a stav zařízení. Každý uživatel je odpovědný za svou činnost na tomto zařízení nebo činnost provozovanou jeho prostřednictvím. Pokud koncové zařízení využívá více uživatelů současně, musí být zajištěna autorizace každého z nich tak, aby bylo vždy možné identifikovat konkrétního uživatele v daném čase. Veškeré instalace, opravy (mimo běžnou údržbu) a administrace koncového zařízení je oprávněna provádět pouze pověřená osoba. Uživatel nesmí zasahovat do programu, dat a technického vybavení počítačové sítě. Jsou zakázány jakékoli změny konfigurace počítačů či jiných prostředků, které by mohly mít vliv

na provoz počítačové sítě. Je možno udělit oprávnění k administraci počítače. V takovém případě je uživatel odpovědný za veškeré programové vybavení, které nebylo nainstalováno

pověřenou osobou. Uživatel musí zároveň evidovat oprávněnost využívání nainstalovaných programů. V případě poruchy nebo problémů se zařízením uvede uživatel problém do tabulky závad a požadavků, která je dostupná na webu školy (zsplana.cz / peadgog / závady ICT). Kromě záznamu může zároveň přímo kontaktovat pověřenou osobu, se kterou si domluví další postup. Pověřená osoba požadavek vyřeší v rámci svých stanovených hodin na údržbu a opravy. Za data uložená na koncové stanici je odpovědný vlastník dat, tj. osoba, která je na toto zařízení uložila nebo modifikovala.

9. Koncová serverová zařízení

Vedení školy určuje podmínky připojení koncového serverového zařízení a jeho provoz. Veškeré nákupy síťových a serverových zařízení schvaluje pověřená osoba a vedení. Správu zařízení zajišťuje pověřená osoba, na kterou mohou být delegována příslušná práva na administraci zařízení a firma spravující počítačovou síť na ZŠ. Za data uložená na serverových zařízeních je odpovědný vlastník dat, tj. osoba, která je na toto zařízení uložila nebo modifikovala.

V Plané nad Lužnicí, 30.6.2020

Mgr. Pavel Grenar
ředitel školy