VOŠZ a SŠZ Ústí nad Labem

Informace a pokyny pro účastníky distanční výuky

Z důvodu zajištění zvýšené ochrany a bezpečnosti osobních údajů našich žáků a studentů má každý uživatel vytvořený emailový účet založený v doméně školy. Ten primárně slouží k práci s výukovými aplikacemi a službami systému Google Workspace.

Emailová adresa je zřízena ve tvaru jmeno.prijmeni@szsvzs.cz. Použití účtu je omezeno dobou studia na naší škole. Po jejím ukončení je účet deaktivován.

Prostřednictvím školního účtu má dotyčný právo přístupu k systémovým aplikacím, které jsou pevně spjaty s doménou školy. Pro výukové potřeby patří mezi stěžejní aplikace Google Classroom, Google Disk, Google Meet a Google Kalendář.

Uživatel se do systému přihlašuje přes stránku https://www.google.cz/. V případě technických dotazů je možné elektronicky kontaktovat správce systému, a to na emailové adrese jiri.stursa@szsvzs.cz.

Veškerá data uživatelů jsou fyzicky uložena a zálohována na území Evropské unie. Při jejich správě se provozovatel systému řídí legislativou platnou v rámci EU. Služba Google Workspace je školám poskytována zdarma, bez reklamních sdělení. Školní obsah není analyzován reklamními systémy Google.

Jediným vlastníkem dat je naše škola (učitelé, zaměstnanci, žáci a studenti). Služba je navržena tak, aby zajišťovala spolehlivé a bezpečné prostředí pro data uživatelů. Poskytovatel provozuje nejnovější technologie. Současně aplikuje doporučené postupy pro zabezpečení síťové infrastruktury a ochranu osobních údajů uživatelů.

Systémy Google Workspace užívají vyspělé systémy zabezpečení a ochrany osobních dat. Mezi ně patří antispamové a antivirové filtry, aplikace Gmail a Google disk. Veškerá komunikace je šifrována pomocí protokolu HTTPS. Přenos souborů EXE je blokován. Systém průběžně automaticky vyhodnocuje a upozorňuje na případná riziková chování uživatelů nebo jiná možná ohrožení.

Systémy Google provádějí kontrolu funkčnosti jednotlivých aplikací za účelem zajištění jejich bezproblémového fungování. Tyto procesy jsou automatické, bez účasti lidí. Administrátorem jsou v prostředí Google Workspace nastaveny společné podmínky pro všechny aplikace. Ty sdílejí identifikaci a autentizaci. Fungují nezávisle na sobě. Systémově jsou definována bezpečnostní nastavení a ochrana před spamem, phishingem a malwarem. Integrace aplikací třetích stran je přesně vymezena. Emailová komunikace užívá pokročilé systémy zobrazování a třídění zpráv.

Google Classroom pracuje s údaji, které slouží pro identifikaci a komunikaci mezi žákem (studentem) a učitelem:

- školní emailová adresa
- jméno a příjmení vyučujícího
- jméno a příjmení žáka (studenta)
- třída (studijní skupina)

Žáci (studenti) mají přístup pouze k zadáním a výsledkům určených jejich osobě. Údaje ostatních jim k dispozici nejsou.

Kompletní materiály může zobrazit pouze vyučující, který je v učebně registrován. Dokumenty jsou uloženy na jeho Google disku v systémové složce Classroom. V ní se automaticky vytvářejí a řadí zadané úkoly a vypracované odpovědi žáků (studentů). Vlastník účtu má oprávnění soubory dále editovat, přesouvat, archivovat či mazat.

Přístup do Google Classroom je možný pouze na základě přijetí pozvánky, kterou odešle ze systému vyučující na školní emailovou adresu žáka (studenta). Vstup do učebny se realizuje pouze prostřednictvím adresy, na kterou byla pozvánka zaslána.

Všichni žáci a studenti jsou průběžně v hodinách informatiky seznamování se zásadami bezpečného chování na internetu, včetně ochrany osobních údajů.

Informovanost je definována těmito oblastmi:

Tvorba a správa hesla

Stěžejním údajem pro přístup do školních aplikací systému Google Workspace je heslo. V případě zadání hesla, které neodpovídá požadavkům na bezpečnost, je toto systémem odmítnuto a uživatel musí zadat heslo jiné.

Základní požadavky na silné heslo:

- Délka hesla musí být minimálně 12 znaků.
- Užití kombinace různých znaků (velká a malá písmena, číslice, symboly). Podporovány jsou pouze znaky standardu ASCII.
- Diakritická znaménka a znaky, které obsahují diakritiku, nejsou podporována.
- Použitý tvar hesla by měl být nahodilý a nesourodý.
- Nelze použít heslo, které bylo v účtu Google již někdy nastaveno.
- Nelze použít heslo, které začíná a končí mezerou.
- Tvar hesla by měl být unikátní.
- Heslo se nesmí nikam zapisovat, ukládat ani sdělovat.
- Nepoužívat trvalé přihlášení do školních účtů.
- Při ukončení práce nebo jejím přerušení se správně odhlásit.
- Nepoužívat stejné heslo pro přihlašování do různých systémů a služeb.
- Nevytvářet hesla obsahující přezdívku uživatele, jeho iniciály, datum narození, údaje z adresy nebo další známé osobní údaje.

Základní uživatelská bezpečnostní opatření na vlastním počítači, mobilním telefonu a dalších zařízeních

- Používání antiviru, antispyware, firewallu.
- Instalace aplikací pouze z ověřených zdrojů.
- Pravidelná aktualizace operačního systému a souvisejících aplikací (mít povolenu automatickou aktualizaci).
- Pravidelná záloha důležitých dat.
- Při obdržení nevyžádané pošty s odkazem a žádostí o zadání osobních údajů (např. bankovnictví) si nejprve ověřit jiným způsobem pravdivost uvedené zprávy. Bez ověření žádné údaje nezadávat.
- Nezadávat žádné osobní údaje na stránkách, které nepodporují zabezpečené připojení.

- Veškerou nevyžádanou poštu hned smazat. Neotevírat ji a neodpovídat. A to ani v případě zájmu o odstranění z distribučního listu. Při odeslání odpovědi získá odesílatel potvrzení, že je účet aktivní. Nejvhodnější je označit zprávu jako spam.

Hlavní zásady užívání školního účtu

Je povoleno:

- Vytvářet a ukládat na sdílená uložiště Google disku pouze materiály související se studiem.
- Při sdílení nastavovat, po dohodě s vyučujícím, různé úrovně oprávnění přístupu.
- Přihlašování k systémům, obsahujícím citlivé informace, provádět pouze prostřednictvím vlastních zařízení přes zabezpečené připojení.
- Používat školní účet pouze pro potřeby výuky.

Je zakázáno:

- Sdělovat přístupy do účtu dalším osobám.
- Zadávat heslo a další údaje v přítomnosti jiných osob.
- Nahrávat na sdílená uložiště Google disku nelegální nebo jinak závadný obsah.
- Provádět registrace na sociálních sítích, které nesouvisejí s výukou.
- Rozesílat nevyžádanou poštu.
- Otevírat a přeposílat podezřelé soubory.
- Sdělovat systémové údaje, které by mohly být případně zneužitelné.

Identita

- Být obezřetní při sdělování osobních údajů.
- Pro stahování aplikací do mobilního telefonu, tabletu atd. používat pouze prověřené portály.
- Při povolení oprávnění aplikacím nejprve posoudit jejich potřebnost. Souhlasy diferencovat. Nepovolat automaticky vše.
- Každou informaci na internetu prověřit více zdroji.
- Upřednostňovat stránky mající zabezpečené připojení.
- Být opatrní při reakcích na příliš výhodné nabídky (např. slevové akce). Jsou podezřelé.

Doporučení pro učitele:

- Používání antiviru, antispyware, firewallu. Tyto systémy mít vždy zapnuté.
- Nutnost pravidelných aktualizací operačního systému a souvisejících aplikací (mít povoleny automatické aktualizace).
- Přihlašovat se pouze prostřednictvím silného hesla.
- Nepoužívat stejné heslo pro přihlašování do různých systémů a služeb.
- Hesla nikam nezapisovat, neukládat, ani nikomu nesdělovat.
- Nepovolovat trvalé přihlášení do školního účtu.
- Při ukončení nebo přerušení práce provést správné odhlášení.
- Důležitá data pravidelně zálohovat.
- Přihlašování k systémům, obsahujícím citlivé informace, provádět pouze prostřednictvím vlastních zařízení přes zabezpečené připojení.

- Podezřelé soubory neotvírat a dále neposílat.
- Dodržovat základní bezpečnostní opatření při pohybu v internetovém prostoru. Věnovat dostatečnou pozornosti odkazům na web. Osobní údaje zadávat pouze na stránkách, které mají zabezpečené připojení.
- Bez ověření nesdělovat osobní nebo systémové údaje.

Uložení žákovských prací na Google disku je zcela bezpečné. Přístup k obsahu má pouze uživatel účtu a případně další osoby, kterým přístup povolí. Proto je vhodný k ukládání studijních materiálů po celou dobu, kdy je třeba s nimi pracovat.

Záznamy a jiné výstupy z výuky je učitel povinen zpracovávat v souladu se zásadami ochrany osobních údajů.

Pokud učitel vytiskne digitální práci žáka, je povinen s tímto dokumentem nakládat v souladu s GDPR. Sem patří i zamezení přístupu osobám, kterým není dokument určen. Po vyhodnocení musí být materiál uložen na bezpečné místo, s dostupností pouze těm zaměstnancům, kteří mají oprávnění s ním pracovat.

Po uplynutí doby potřebné pro archivaci, musí být dokument předán ke skartaci, kterou provede pověřená osoba. Ta zajistí, aby do doby fyzického provedení skartace nebylo možné s materiálem jinak nakládat.

Základní zásady pro výuku, zkoušení a testování

- Při výuce prostřednictvím videokonference je doporučeno se posadit tak, aby za zády přednášejícího bylo pouze neutrální pozadí, ve kterém by nebyl žádný další pohyb osob.
- Je možné nastavit elektronické rozmazání pozadí.
- Při distribuci vzdělávacích materiálů upřednostňovat sdílené obrázky, prezentace a další materiály.
- Online hodinu je možné nahrávat. Záznam, včetně výstupů z výuky, pak ukládat na zabezpečené důvěryhodné úložiště.
- Při testování je vhodné, pokud to typ látky umožňuje, zadávací dokument uložit do pdf, se záznamem data a času vytvoření.
- Při vyplňování údajů k jednotlivým hodinám je vhodné zadávat co nejméně detailů týkajících se konkrétních osob.
- Při online zkoušení je vhodné dávat přednost testování v malých skupinách, případně individuální komunikaci s každým žákem (studentem).