Správa o činnosti pedagogického klubu

1. Prioritná os	Vzdelávanie
2. Špecifický cieľ	1.2.1 Zvýšiť kvalitu odborného vzdelávania a prípravy reflektujúc potreby trhu práce
3. Prijímateľ	Obchodná akadémia Liptovský Mikuláš
4. Názov projektu	Zvýšenie kvality odborného vzdelávania a prípravy na Obchodnej akadémii Liptovský Mikuláš
5. Kód projektu ITMS2014+	312011AGY1
6. Názov pedagogického klubu	Klub IKT
7. Dátum stretnutia pedagogického klubu	07. 06. 2022
8. Miesto stretnutia pedagogického klubu	OALM
9. Meno koordinátora pedagogického klubu	Ing. Stanislav Peniaško
10. Odkaz na webové sídlo zverejnenej správy	www.oalm.edupage.org

11. Manažérske zhrnutie:

Na stretnutí Klubu IKT sme sa zaoberali problematikou používania informačno-komunikačných technológií z hľadiska bezpečnosti.

V prvej časti stretnutia nám Ing. Peniaško najprv objasnil základnú terminológiu súvisiacu s preberanou témou. Následne upriamil našu pozornosť na dôležitú publikáciu (NE)BEZPEČNE V SIETI. Tento manuál vysvetľuje nielen prehľadne teóriu, ale ponúka pre učiteľov a ostatných pedagogických pracovníkov aj základnú metodiku pre rozvoj kritického myslenia študentov v online priestore.

V druhej časti stretnutia sme vzájomne diskutovali o tom, ako pracujeme so spomínanou problematikou v edukačnom procese a v akej miere ju aplikujeme vo svojej práci. Každý z nás bližšie ozrejmil ostatným členom hlavne tie oblasti, ktorým sa vo väčšej miere venuje vo svojich vyučovacích predmetoch. Napríklad o médiách nás informovala Mgr. Dvorščáková v rámci predmetov nemecký jazyk a projektové vyučovanie praktikum. O téme digitálneho občianstva aplikovaného v predmetoch informatika a digitálna kancelária nás informoval Ing. Peniaško a pod.

V poslednej časti stretnutia boli účastníkmi klubu navrhnuté závery a odporúčania pre prácu súvisiacu s faktormi, ktoré ovplyvňujú správanie vo virtuálnom i offline priestore. Taktiež sme si v závere rozdelili tematické oblasti, ktorým by sme sa mohli vo svojich vyučovacích predmetoch podrobnejšie venovať.

Kľúčové slová:
mediálna gramotnosť, kritické myslenie, bezpečné využívanie internetu, kyberšikanovanie, digitálne občianstvo, manuál, výchovno-vzdelávací proces

12. Hlavné body, témy stretnutia, zhrnutie priebehu stretnutia:

V súčasnej dynamickej dobe, ktorá je charakteristická neustálym rozmachom rôznych technológií, je veľmi potrebné uvedomiť si aj dôležitosť problematiky bezpečnostných aspektov používania informačno-komunikačných technológií. K tomu, aby pedagógovia mohli pracovať v tomto smere so študentmi, je nevyhnutné, aby porozumeli základným pojmom a vedeli nadobudnuté vedomosti a skúsenosti realizovať v praxi.

Obsahovo stretnutie klubu bezprostredne a plynule nadväzovalo na predchádzajúce, ktoré sa taktiež dotýkalo problematiky bezpečného využívania internetu a digitálnych technológií. Kým v predošlom stretnutí sme sa podrobnejšie venovali hlavne mediálnej gramotnosti, hlavnými bodmi tohto stretnutia boli predovšetkým kritické myslenie, kyberšikanovanie a jeho druhy, digitálne občianstvo i praktické zážitkové aktivity k riešeným témam.

Ing. Peniaško nám na začiatku stretnutia ozrejmil základné teoretické pojmy a tematické oblasti.

Kritické myslenie

Tento pojem možno charakterizovať z viacerých aspektov. Kritickým myslením môžeme rozumieť komplex myšlienkových operácií, ktoré začínajú informáciou, ktorá aktivizuje zvedavosť. Ide o schopnosť nepodliehať prvému dojmu, ktorý môže byť založený na iracionálnom uvažovaní. Je to myslenie hľadajúce fakty a dôkazy. Spočíva v tom, že zhodnotíme a posúdime to, ako vidíme alebo počujeme fakty či určitú situáciu. Ide o vytvorenie si vlastného názoru.

Ku ***kľúčovým schopnostiam*** kriticky mysliaceho človeka patrí schopnosť:

- ***pozorovať*** – sústredene vnímať, sledovať informácie s cieľom poznať ich, získať vedomosti o ich obsahu, zdroji, výpovednej hodnote;
- ***interpretovať*** – výklad prijatých informácií a vysvetlenie ich významu, príčiny, prečo vznikli a cieľu, ktorý sledujú;
- ***analyzovať*** – rozbor informácie ako celku na jednotlivé časti, rozkladanie obsahu informácie;
- ***odvodzovať a vyvodzovať*** – dedukcia rôznych informácií, myšlienok a súvislostí z textu, ktoré v ňom nie sú jednoznačne formulované a vyvodenie významu alebo súvislosti medzi myšlienkami; stanovenie hlavnej myšlienky;
- ***hodnotiť*** – posúdenie pravdepodobnosti, že získané informácie sú skutočné a pravdivé; určenie úplnosti a zrozumiteľnosti daných informácií.

Kritické myslenie je súčasným nárastom vplyvu rôznych dezinformácií a propagánd potrebné podporovať a rozvíjať u žiakov už od ranného veku. Pedagóg, ktorý chce rozvíjať takéto myslenie, by mal poznať základné pojmy spojené s touto problematikou. Medzi tieto základné pojmy patria napríklad: ***manipulácia*** (snaha ovládať myslenie druhej osoby alebo skupiny osôb), ***spam*** (nevyžiadaná, hromadne rozosielaná správa, ide o zneužívanie elektronickej komunikácie, hlavne e-mailu), ***hoax*** (prostredníctvom internetu šírená správa, ktorá vyzýva, aby bola preposielaná ďalším užívateľom systému), ***dezinformácia*** (zámerne vytvorená, skreslená alebo chybná informácia, ktorej cieľom je pomýlenie alebo zavádzanie adresáta), ***demagógia, propaganda*** (charakteristická dlhodobým pôsobením, je koncepčná a má za cieľ ovplyvnenie myslenia, postojov a konania), ***konšpirácia*** (sprisahanie, ilegálna činnosť, komplot), prípadne ***konšpiračná teória.***

Bezpečné využívanie internetu a digitálnych technológií, kyberšikanovanie

Kyberšikanovanie

Je nežiadúcim sociálno-psychologickým fenoménom a je jednou z foriem šikanovania. Pod týmto pojmom môžeme rozumieť zneužívanie informačných a komunikačných technológií (mobilné telefóny, smartfóny, internet) s cieľom zámerného ublíženia druhým osobám.

Pri kyberšikanovaní môže ísť o viacero spôsobov ubližovania. Častokrát sa uskutočňujú súčasne. K základným ***druhom kyberšikanovania*** patrí:

- ***Znevažovanie vo verejnom online priestore*** - útočníci obeť ponižujú napr. na sociálnych sieťach, v četovacích skupinách znevažujúcim obsahom, ktorý obeť zosmiešni alebo poškodí jej dobré meno.

- ***Provokovanie online*** - útočníci zámerne provokujú svoje obete správami a príspevkami s urážlivým, nepravdivým alebo vulgárnym obsahom, ktorý púta pozornosť obete. Týmto spôsobom útočník vťahuje obeť do nekorektného dialógu a dokazuje tak svoju moc.

- ***Zneužitie online identity*** - agresor sa prostredníctvom prelomenia hesla dostane napr. do profilu na sociálnej sieti obete a zneužije ho. Útočník následne môže upravovať pôvodné správy, komunikovať s kontaktmi v mene obete, zverejňovať príspevky poškodzujúce obeť a pod. Takto ukradnutý profil agresorovi slúži ako nástroj pre manipulovanie a vydieranie.

- ***Outing*** – agresor zverejní na internete súkromné informácie obete bez jej súhlasu, napr. intímne fotografie, obrázky, rôzne videá.

- ***Online vylúčenie*** – predstavuje zámerné vylúčenie obete z online komunity, napr. zo sociálnych sietí, četovacej miestnosti, z diskusií, hráčskej komunity a pod.

- ***Cyberstalking*** - agresor obeť obťažuje a prenasleduje, a tým narúša jej pocit bezpečia. Znepríjemňuje jej život zahlcujúcimi interakciami, napr. spamovaním, opakovaným posielaním fotografií, správami v četoch a pod. Tento typ pozornosti je pre obeť obťažujúci kvôli jej intenzite a frekvencii.

- ***Happy slapping („fackovanie pre zábavu")*** - ide o prepojenie šikanovania s kyberšikanovaním. Podstata spočíva vo fyzickom útoku na obeť a nahraní celej udalosti na mobilný telefón. Následne útočník zverejní nahrávku na internete, prípadne ju iným spôsobom elektronicky šíri ďalej. Agresorom pri tomto druhu býva častokrát skupina.

Veľmi dôležitú úlohu v súvislosti s kyberšikanovaním zohráva samotná ***prevencia,*** ktorá by mala byť založená na:

- zvyšovaní informovanosti učiteľov i študentov o kyberšikanovaní;
- zvyšovaní vedomostí a zručností v súvislosti s bezpečným používaním internetu;
- zlepšovaní vzájomných vzťahov medzi žiakmi v škole;
- učení ako pracovať so svojimi emóciami, ako sa vysporiadať so záťažovými situáciami;
- rozvoji sociálnych zručností a sebapoznania.

Základné pravidlá bezpečného zdieľania na internete

- čokoľvek je zdieľané na internete, ostáva tam už navždy bez ohľadu na to, či to bolo zmazané;
- odporúča sa používať sociálne siete primerané pre daný vek a ktoré sa vyznačujú vyššou bezpečnosťou;

- nastaviť si profil na sociálnych sieťach ako súkromný;
- nezdieľať príliš veľa detailov, neuvádzať v profile svoje osobné informácie; nezdieľať nič citlivé, kontroverzné; nezdieľať čísla ani fotografie rôznych osobných dokladov, telefónne čísla, adresu, zmluvy a oficiálne dokumenty (napr. vysvedčenie a pod.);
- pravidelne si kontrolovať členstvo v skupinách;
- na podozrivé správy a linky sa odporúča neklikať.

Bezpečnosť prehliadača

Základom bezpečného používania internetu je výber a používanie bezpečného a aktuálneho webového prehliadača. V prípade, že máme nainštalovaných viacero prehliadačov, je potrebné aktualizovať všetky. Prehliadače obvykle poskytujú používateľovi aj možnosť „Bezpečné prehliadanie webu". V tomto móde nás chránia pred kyberkriminalitou akou je napr. phishing, krádež hesla a citlivých údajov. Aktivovať si ho môžeme v sekcii „Nastavenia". Tento mód prehliadača hlási, keď sa používateľ snaží pripojiť na také stránky, ktoré vyzerajú podozrivo alebo je už známe, že šíria škodlivý kód. Na základe tejto informácie sa ľahšie dozvieme, kedy môžeme byť ohrození kyberkriminalitou.

Digitálne občianstvo

Digitálnym občianstvom môžeme rozumieť celkové správanie a pohybovanie sa v online priestore. Podstata takéhoto občianstva spočíva vo zvyšovaní vedomostí a na aktívnom človeku, ktorý používa digitálne technológie vedome a bezpečne, zúčastňuje sa na verejnom živote, zapája sa do diania v spoločnosti s využitím informačno-komunikačných technológií. Znamená kompetentné a pozitívne používanie rôznych digitálnych technológií (tvorba, práca, zdieľanie, socializovanie, komunikovanie). Môžeme povedať, že digitálne občianstvo je postavené na troch ***základných pilieroch,*** ktorými sú:

- ***bezpečnosť*** (bezpečne, 1. pilier);
- ***participácia*** (jednotlivec/skupina ako aktívny účastník procesu: 2. pilier);
- ***online*** (s využitím prepojených digitálnych technológií: 3. pilier).

Pre ***digitálneho občana*** sú charakteristické nasledovné ***zásady:***

- ***aktívnosť*** občana – sám aktívne vyhľadáva informácie online;
- ***angažovanosť*** občana vo ***verejnom živote*** a ***pre spoločné dobro*** – zaujíma sa o dianie v spoločnosti, vykonáva dobrovoľnícku činnosť;
- ***znalosť ako sa pohybovať online bezpečne*** - ovláda základné princípy bezpečnosti;
- ***pomoc ostatným získavať pozitívne digitálne skúsenosti*** – prenáša svoje skúsenosti ďalej;
- ***vedomý prístup a fakt,*** že každý ***čin má*** svoj ***následok*** – používateľ internetu dobre pozná obsah publikovaného, prehodnocuje pravdivosť informácií;
- ***kompetentný*** a ***znalý používateľ*** technológií a internetu – pozná bezpečnostné nastavenia sociálnych sietí, softvérov, aplikácií a pod.;
- ***etický prístup*** – nezdieľa zakázané informácie, myslí na dôsledky svojho správania.

V ďalšej časti stretnutia sme komunikovali o tom, ako pracujeme s vyššie uvedenými tematickými oblasťami v rámci svojich vyučovacích predmetov a čomu by sme mali venovať zvýšenú pozornosť. Vzájomne sme si vymenili nadobudnuté poznatky a skúsenosti, cenné rady i rôzne postrehy.

V tretej časti stretnutia klubu boli jednotlivými členmi vyvodené závery a odporúčania pre prax.

13. Závery a odporúčania:

Všetci účastníci klubu IKT sa jednoznačne zhodli na tom, že je veľmi potrebné neustále vzdelávanie sa pedagógov v riešenej problematike prostredníctvom rôznych kurzov, seminárov, webinárov, školení, samoštúdiom a pod.
Taktiež je nevyhnutné, aby mediálna výchova, kritické myslenie a počítačová gramotnosť boli zahrnuté vo vzdelávacom programe. Rovnako je dôležité, aby vzdelávacie inštitúcie aktívne spolupracovali so žiakmi ako s partnermi, načúvali im. Žiaci by nemali byť iba pasívnymi prijímateľmi informácií a vedomostí sprostredkovanými pedagógmi a odbornými pracovníkmi, ale mali by sa aktívne zapájať, napr. do rovesníckych programov, prípadne spolupracovať s budúcimi zamestnávateľmi.
Taktiež rodičia by mali chápať potrebu k výchove a vzdelávaniu svojich detí, zapájať sa do rôznych aktivít realizovaných v rámci formálneho a neformálneho vzdelávania. Vzťah medzi rodičmi a deťmi z hľadiska digitálneho občianstva je veľmi potrebný.
Jedným z nástrojov, ktorý sa zaujímavým spôsobom venuje práve týmto témam, je prehľadný manuál s názvom (NE)BEZPEČNE V SIETI. Odporúčame ho preštudovať všetkým pedagógom, vychovávateľom, rodičom a pod. Okrem zrozumiteľného vysvetlenia základných teoretických pojmov ponúka aj viaceré pútavé zážitkové aktivity, ktoré možno efektívnym spôsobom využiť vo výchovno-vzdelávacom procese. Súčasne aj táto správa o činnosti klubu môže slúžiť ako základné východisko pre prácu so spomínanou problematikou.

14. Vypracoval (meno, priezvisko)	Mgr. Martina Mikóczyová
15. Dátum	07. 06. 2022
16. Podpis	
17. Schválil (meno, priezvisko)	Ing. Stanislav Peniaško
18. Dátum	07. 06. 2022
19. Podpis	