POLITICA ESAFETY GPPO1

siguranţa în practica de predare

Nr. 1568 din 27.09.2024
Reactualizată în data de 03.09.2024

Membrii Comisiei eSafety:
Prof. Țuca Maria - Responsabil
Director Albinaru Maria Corina - membru
Prof. Feloiu Ramona Georgeta - membru
Prof. Manda Cristina - membru
Prof. Vărgăluță Maria Mălina – membru

OPIS

INTRODUCERE

GPPO1 a considerat că este oportun să adopte o politică de securitate electronică pentru a ține pasul cu momentele din societatea cunoașterii actuale în care își desfășoară activitatea, în special în ceea ce privește formarea cetățenilor viitorului, destinat să trăiască într-un mediu în care totul este gestionat prin utilizarea tehnologiilor informației și comunicațiilor (TIC).

Aceste tehnologii devin activatoare, zilnice, obișnuite, în slujba GPPO1 și a tuturor mediilor sale, implicând atât activități care vizează instruirea, cât și învățarea și administrarea, cu implicații extinse pe teritoriu.

Cu acest document dorim să reglementăm utilizarea Internetului pentru a face responsabilii tuturor utilizatorilor GPPO1, astfel încât să garanteze confidențialitatea în cadrul birourilor complexe și secretariale. Ghidurile naționale subliniază abilitățile digitale ale prescolarilor, care trebuie să știe să se orienteze în multiplele posibilități oferite de Web, analizând critic materialele disponibile, schimbând informații și experiențe într-un mod conștient și responsabil.

În acest sens, este necesar să informați și să instruiți membrii GPPO1, în special prescolarii, despre posibilele riscuri și să oferiți măsuri care să le prevină, permițându-le să beneficieze în siguranță de oportunitățile oferite de Internet și TIC. La sfârșitul documentului este introdus un glosar pentru o mai bună înțelegere.

Politica de siguranță electronică va fi revizuită și actualizată periodic pe baza unor posibile variații ale standardelor, echipamentelor tehnologice și protocoalelor gradinitei.

OBIECTIVUL POLITICII E-SAFETY

Obiectivul acestui document este de a informa utilizatorii pentru a garanta o utilizare corectă și responsabilă a echipamentelor informatice furnizate GPPO1, în conformitate cu legislația în vigoare. Prin urmare, este esențial să cunoaștem regulile și procedurile comportamentale pentru utilizarea TIC în mediul școlar, măsurile de prevenire și cele pentru detectarea și gestionarea problemelor legate de utilizarea tehnologiilor digitale.

Toți utilizatorii trebuie să cunoască riscurile la care sunt expuși de fiecare dată când navighează pe internet: există, de fapt, posibilitatea ca în timpul lucrului online să poți contacta accidental cu materiale necorespunzătoare și/sau ilegale. Prin urmare, GPPO1 promovează adoptarea de strategii care limitează accesul la site-uri și / sau aplicații ilicite. În acest context, profesorii sunt responsabili de îndrumarea prescolarilor în activități online la școală și de a indica reguli clare de conduită pentru o utilizare critică și conștientă a internetului acasă, pentru a preveni apariția unor situații potențial periculoase.

Profesorii, conștienți de faptul că este imposibil să se garanteze o navigare total lipsită de riscuri în mediile școlare, nu își pot asuma responsabilitatea pentru accesul accidental și / sau necorespunzător la site-uri ilicite sau regăsirea și utilizarea materialelor necorespunzătoare.

SPAȚII VIRTUALE DISPONIBILE ÎN GPPO1

În GPPO1, calitatea și cantitatea instrumentelor sunt în implementare continuă:

- furnizarea de noi instrumente IT este un obiectiv prioritar, pornind de la prezența IWB în toate clasele;

- laboratoarele de calcul, prezente în diferitele plexuri, sunt echipate cu conexiune la internet prin WIFI și rețea de cablu, stații de lucru pentru PC pentru profesori și proiectoare video;
- secretariatul, în conformitate cu legislația actuală, atinge progresiv obiectivul dematerializării complete; o atenție deosebită este acordată modernizării echipamentelor IT, întreținerii și actualizării constante a rețelei IT și modernizării serviciilor digitale ale GPPO1-familie-prescolari. Reprezentanților diferitelor laboratoare au sarcina de a verifica funcționarea și respectarea regulamentului. Profesorii și personalul ATA trebuie să utilizeze instrumentele prezente în școală cu cel mai mare respect, respectând reglementările actuale și reducând la minimum risipa resurselor disponibile. Profesorii trebuie să utilizeze criteriile TIC în activitățile educaționale și au sarcina fundamentală de a împuternici prescolarii să-i conștientizeze cu privire la importanța protejării unui bun comun, prin reguli de utilizare corectă.

STRATEGII PENTRU GARANŢIA SECURITĂŢII TIC

GPPO1 oferă următoarele strategii pentru a asigura securitatea online:

1. Analizați nevoile de formare ale cadrelor didactice și promovează cursuri de instruire cu privire la utilizarea sigură și responsabilă a TIC și Web, atât în utilizarea lor privată, cât și la școală;
2. Să implementeze, eventual în colaborare cu experți externi, întâlniri pentru a prezenta tuturor membrilor comunității școlare:
   - *Modalități corecte de utilizare a Web-ului,*
   - *Protecția minorilor pe internet și pe rețelele sociale,*
   - *Prevenirea și contrastul fenomenul de utilizare cibernetică responsabilă a web-ului;*
3. Informează despre problemele psihopedagogice legate de utilizarea Web-ului;
4. Organizează rețelele plexurilor în subrețele dedicate diferitelor tipuri de utilizatori; • creează profiluri pentru diferite tipuri de utilizatori;
5. Monitorizează periodic sistemul informatic, în special pentru ceea ce privește utilizarea Internetului, istoricul, cookie-urile ..., de către managerii laboratorului, informând în prealabil utilizatorii controlului;
6. Solicită, după caz, intervenția companiilor IT care se ocupă de întreținerea și asistența dispozitivelor cu acțiuni la fața locului sau de la distanță;
7. Garantează prezența constantă a unui profesor în timp ce utilizează internetul sau alte TIC;
8. Instalați firewall-ul pe acces la Internet;
9. Actualizați în mod regulat sistemul de operare, aplicația software și antivirus; scanează dispozitivele unde se poate suspecta viruși sau malware;
10. Utilizați stick-uri USB, CD, DVD sau alte dispozitive externe personale numai dacă au fost autorizate anterior de profesorul responsabil;
11. Organizează un sistem pentru monitorizarea eventualelor probleme întâmpinate în timpul utilizării TIC sau a rețelei și oferă planuri de acțiune pentru rezolvarea celor mai frecvente;
12. Evidențiază interdicția de a adopta comportamente contrare acestui regulament și legislației actuale, cum ar fi, de exemplu:
    - *Sau descărcați fișiere cu drepturi de autor și încalcă legile privind drepturile de autor;*
    - *Sau vizitați site-uri care nu au legătură cu activitățile educaționale, utilizați Web-ul pentru interese private și personale;*
    - *Sau modificați parametrii de protecție ai dispozitivelor utilizate.*

GPPOstroveni 1
Oraş Râmnicu Vâlcea, Judeţ Vâlcea
Str. Aleea Teilor Nr. 5,
cod poştal 240077, tel: 0350414817
e-mail: gppostroveni1@gmail.com
Site: https://gradinitaostroveni1.ro

FOLOSIREA DISPOZITIVELOR DETAȘABILE

Dispozitiv detașabil înseamnă orice dispozitiv media care poate fi citit și/sau inscripționat de către utilizatorul final și mutat de la un computer la altul fără să producă modificări computerului respectiv. Printre aceste tipuri de dispozitive se numără aparatele ce conţin memorii flash, cum ar fi aparate foto, MP3 playere, hard disk-uri portabile, CD-uri, DVD-uri și stick-uri USB. Utilizarea dispozitivelor de stocare detaşabile este o sursă bine-cunoscută de infecții malware şi este direct legată de scurgerea de informații sensibile în multe organizații. Este necesar să se ia măsuri corespunzătoare pentru a reduce la minimum riscul de scurgere sau de expunere a informațiilor sensibile și pentru a reduce riscul infecţiilor malware pe computerele școlii.

Dezvoltaţi în cadrul Politicii de Utilizare Acceptabilă reguli de bază privind folosirea dispozitivelor detaşabile de stocare pe computerele școalii.

Instalați un sistem de protecție antivirus pe toate computerele din rețeaua școlară și adoptaţi o practică constantă la nivel de școală în ceea ce priveşte protecția împotriva virușilor. Un fișier infectat de pe un dispozitiv de stocare amovibil ar putea infecta întreaga rețeau școlară.

Solicitaţi membrilor personalului și elevilor să scaneze toate dispozitivele detaşabile împotriva programelor malware înainte de a le utiliza și oferiţi-le suficiente îndrumări pentru a efectua cu succes această procedură.

Permiteţi utilizarea dispozitivelor mobile numai când sunt necesare în vederea îndeplinirii sarcinilor școlare. Elevilor și membrilor personalului nu trebuie să li se permită, de exemplu, să-şi conecteze aparatul foto sau un MP5 player-ul la un computer din reţeaua şcolii, cu excepția cazului în care trebuie să facă acest lucru în cadrul unei sarcini specifice pe care au primit-o.

Încurajaţi personalul și elevii să salveze fișiere pe dispozitivele mobile pe care le folosesc pe computerele şcolii doar în scopuri educaționale.

Personalul ar trebui să evite stocarea datelor sensibile ale elevilor și ale altor membrii ai personalului pe dispozitive detaşabile cu excepția cazului în care acest lucru este necesar în vederea executării sarcinilor ce le revin, deoarece există întotdeauna riscul ca aceste dispozitive cu informații personale pe ele să fie furate sau pierdute.

Instituiţi o procedură oficială de gestionare a incidentelor în cazul unor infectii malware prin utilizarea unui dispozitiv mobil sau în cazul pierderii unui dispozitiv. Aceasta din urmă este deosebit de importantă dacă dispozitivul conține informații sensibile despre elevi sau personal.

Fără a aduce atingere strategiilor sistematice puse în aplicare de GPPO1 la care se face referire în paragraful anterior și așa cum este prevăzut în norme, fiecare utilizator conectat la rețea trebuie:

- să respecte prezentul regulament și legislația în vigoare;
- protejarea propriei vieți private, a prescolarilor și a altor utilizatori adulți pentru a nu divulga informațiile private conținute în documentele digitale la care are acces;
- respectă netiquette, regulile partajate care reglementează relația dintre utilizatorii rețelei, în contact prin site-uri, forumuri, poștă, bloguri, grupuri de știri ... Comportament legat de activitățile care urmează să fie organizate: profesori, prescolari și părinți.

PROTEJAREA DISPOZITIVELOR ÎMPOTRIVA MALWARE-ULUI

Malware înseamnă software dăunător care a fost proiectat cu scopul accesării unei rețele sau unui sistem de computere fără consimțământul proprietarului şi poate include viruși, viermi și spyware. Odată instalat, malware-ul cauzează de obicei rezultate nedorite, care pot varia de la a fi pur și simplu intruziv sau enervant până la a compromite informații cu caracter personal în sistem sau până la a fi pur și simplu distructiv. Malware-ul ajunge de obicei în sistemul IT al unei școli prin intermediul spam-ului, descărcării de fișiere contaminate sau prin intermediul dispozitivelor mobile infectate (USB, hard disk extern, telefon mobil, etc.).

Ghid
Instalați firewall-uri și sisteme de protecție anti-virus și actualizaţi-le pentru a evita breșele de securitate.
Blocaţi site-urile nedorite și ferestrele de tip pop-up prin personalizarea setărilor de securitate ale browser-ului web utilizat pe computerele şcolii. Explicați elevilor de ce anume se face acest lucru și precizaţi că prin aceasta se urmăreşte protecția lor.
Creați un protocol care să fie aplicat cu rigurozitate cu privire la utilizarea Internetului și verificarea mail-urilor personale pe computerele şcolii.
Furnizaţi personalului o formare de bază în ceea ce priveşte depistarea potențialelor fișierele infectate și practicile sigure atunci când descarcă fișiere sau utilizează dispozitive portabile.
Nu permiteţi elevilor să folosească dispozitive portabile pentru a descărca fișiere de pe computerele şcolii; în cazul în care acest lucru este permis trebuie să fie instruiţi să scaneze mai întâi toate fișierele împotriva malware.
Desemnați o persoană de contact instruită să se ocupe de toate problemele legate de malware și instituiţi o procedură oficială de gestionare a incidentelor.

Parole sigure

Parolele oferă puncte unice de intrare în sistemul școlar de computere și trebuie aplicate cu rigurozitate câteva reguli de bază referitoare la securitatea acestora.

O parolă este un element important care deschide accesul la sistemul dvs.; evitaţi acordarea de parole standard de prim acces noilor utilizatori.
Asigurați-vă că sistemul atribuie o parolă diferită fiecărui nou-venit și solicitaţi-le să genereze propria parolă prima dată când accesează sistemul școlar.
Amintiţi personalului și elevilor cele 4 reguli de aur ale unui parole sigure:
Trebuie să fie lungă și complexă. Ideal trebuie să conţină între 10 și 14 caractere;
Folositi un amestec de numere, simboluri, litere mari şi litere mici și semne de punctuație;
Folosiți metode mnemonice care să vă ajute să vă amintiţi parola, de exemplu un acronim pentru o frază, cum ar fi "Fiica mea, Harriet, este o bună jucătoare de tenis" devine FMhEObjDt sau Imi place să cânt in ploaie in fiecare zi! devine iPScipIFZ!;
Nu folosiți niciodată informații personale de identificare în parolă. Acestea includ nume, zile de naștere, animale de companie, adrese de străzi, şcoli, numere de telefon, numerele de înmatriculare etc. Acestea vor fi primele presupuneri pentru oricine încearcă să obțină acces la contul dvs.

parolă este ca o periuţă de dinţi, nu trebui folosită în comun și trebuie să fie schimbată frecvent! Dacă utilizatorii simt totuşi nevoie să scrie parola, aceasta nu trebuie să fie ţinută în apropierea dispozitivului la care oferă acces. Încorporaţi regulile esențiale privind gestionarea parolelor în Politica de utilizare acceptabilă, invitaţi profesorii să consulte frecvent PUA la clasele lor ca o reamintire a ceea ce au semnat.

POLITICI DE ESAFETY ÎN ŞCOALĂ

Politicile de eSafety ale şcolii s-au dezvoltat rapid, deoarece părțile interesate pot accesa în prezent Internetul într-o multitudine de moduri în incinta școlii. Tehnologiile digitale fac parte din viața noastră de zi cu zi. Pentru a ne asigura că oportunitățile disponibile prin intermediul tehnologiilor digitale sunt valorificate cum se cuvine de către copiii noștri, aceştia trebuie să le cunoască și să înțeleagă cum să le folosească, acum mai mult ca niciodată. Pentru a ne asigura că acest lucru se face în cel mai sigur mediu posibil, fie acasă, fie la școală sau când ies în oraş singuri sau cu prietenii lor, toate școlile trebuie să aibă o politică clară și concisă în care să se acorde atenție tuturor aspectelor eSafety.

Ghid

Deşi siguranţa este responsabilitatea fiecărui profesor, de politica de eSafety a şcolii trebuie să se ocupe o singură persoană responsabilă cu implementarea, revizuirea și acţiunile necesare. Această persoană, numită uneori coordonatorul eSafety, va supraveghea punerea în aplicare și monitorizarea politicii eSafety şi va raporta Comitetului eSafety și directorului cel puțin o dată pe an sau mai des, în lumina oricăror noi evoluții semnificative în utilizarea tehnologiilor, noi amenințări la adresa eSafety sau în cazul în care au avut loc incidente.

Politica de eSafety a şcolii trebuie să țină pasul cu evoluțiile digitale și noile tendințe relevante pentru siguranța și securitatea personalului, elevilor și părinților, precum și pentru reputația și viitorul școlii.

Legislația la care se face referire în politica eSafety a școlii trebuie să fie citată în timpul şedinţelor referitoare la subiectele acoperite de către această politică, de exemplu, comportamentul adecvat, schimbul de informații sau imagini ilegale etc.

Politica de eSafety a şcolii trebuie să fie fermă și coerentă în domeniile-cheie eSafety, încurajând în același timp conștientizarea de către elevi a folosirii sănătoase a tehnologiilor online.

Potrivită scopului – politica de eSafety a şcolii ar trebui să fie în concordanţă cu PUA și cu alte politici legate de siguranță din cadrul școlii, de exemplu, cele privind protecția copilului, comportamentul anti-social sau anti-bullying-ul.

Încurajarea implicării părților interesate - se recomandă implicarea tuturor părților interesate în crearea politicii: elevi, cadre didactice, părinți și membri ai comunității mai largi. Acest lucru va reprezenta o asigurare că toate grupurile au drept de proprietate asupra anumitor părți ale politicii și, ca urmare, sunt mai dispuse să adera la ea.

Claritate și concizie - limbajul folosit pentru redactarea politicii de eSafety a şcolii trebuie să fie non-tehnic şi uşor de înţeles, cu îndrumări clare care să ofere o asigure că tot personalul și elevii știu ce se așteaptă de la ei.

GPPOstroveni 1
Oraş Râmnicu Vâlcea, Judeţ Vâlcea
Str. Aleea Teilor Nr. 5,
cod poştal 240077, tel: 0350414817
e-mail: gppostroveni1@gmail.com
Site: https://gradinitaostroveni1.ro

PUA PROFESORI

În timpul predării activitate pe care fiecare profesor le poate folosi instrumentele disponibile și trebuie:

- Să citească, să înțeleagă și să respecte această politică;
- Să aibă grijă de instrumentele furnizate, în special prin oprirea corectă a tabletelor, pc-urilor, a dispozitivelor lim și a proiectoarelor video la sfârșitul perioadei de utilizare, așezându-le în locul prevăzut;
- Profesorul din ultima oră de lecții trebuie să verifice dacă toate instrumentele sunt oprite și stocate corect;
- Accesați personal la registrul electronic prin intermediul tabletei sau al pc-ului în utilizare și completați zona rprescolarantă; tableta sau computerul trebuie păstrate la îndemâna prescolarilor; va fi responsabilitatea profesorului de a nu lăsa dispozitive nesupravegheate în timpul mișcărilor clasei în alte locuri ale GPPO1;
- Păstrează secretul certificatelor de acces la registrul electronic și la zona restrânsă a GPPO1;
- Să nu dezvăluie prescolarilor acreditările de acces la rețeaua wifi rezervată profesorilor
- Lăsați neschimbate setările dispozitivelor școlare;
- Completați registrul de utilizare pentru a asigura trasabilitatea activităților și întreținerea în stare bună a echipamentului tehnologic utilizat, raportând prompt managerilor orice defecțiuni, conform procedurilor prevăzute;
- Nu salvați fișierele care conțin date personale și / sau date sensibile pe dispozitivele utilizate;
- Nu memorați acreditările, e-mailurile, fișierele personale pe dispozitive;
- Asigurați-vă că v-ați deconectat de la fiecare serviciu înainte de a părăsi stația;
- Salvați fișierele de lucru în dosarele personale sau de clasă și nu pe desktop; fișierele care nu sunt salvate în acest mod vor fi șterse de către managerul de echipamente;
- Să folosească laboratorul care așteaptă la ora convenită la începutul anului, să semneze registrul de acces completând câmpurile necesare, să raporteze orice defecțiuni constatate înainte, în timpul sau la sfârșitul activității desfășurate;
- Să permită accesul prescolarilor la atelier doar dacă este însoțit de profesori;
- Înainte de a părăsi laboratorul, asigurați-vă că toate calculatoarele au fost oprite corect; dacă este necesar, completați formularul pentru raportarea problemelor;
- Verificați utilizarea corectă a laboratorului și a instrumentației, asigurându-vă că nu sunt introduse alimente sau băuturi;
- Aplicați aceleași precauții în sălile de clasă amplificate de tehnologie;
- Asigurați-vă că accesul prescolarilor la rețea este întotdeauna supravegheat, informați-i despre riscurile la care pot fi expuși și utilizarea corectă a rețelei (motoare de căutare, platforme online, clase virtuale);
- Previzualizați site-urile care vor fi propuse în avans, verificând cu atenție siguranța și respectarea drepturilor de proprietate intelectuală;
- Îndrumă prescolarii în cercetarea online: oferă obiective clare, propune adrese web, cuvinte cheie pentru cercetare, preferă site-urile instituționale, create special pentru predare; să urmăriți, în timpul navigării, că toată lumea folosește corect net, oferind indicații constante cu privire la ceea ce este necesar de netiquette;
- Raportează managerilor utilizarea site-urilor de internet care nu sunt compatibile cu politica educațională a GPPO1. Prescolarii în timpul activității de predare, prescolarii trebuie:
- Să citească, să înțeleagă și să respecte această politică;

- Accesați laboratorul informatic numai dacă este însoțit de profesori și urmați instrucțiunile furnizate privind utilizarea tic;
- Să acceseze mediile de lucru cu propriile lor credențiale, fără să le divulgă și să stocheze fișierele lor într-o manieră ordonată, astfel încât să fie ușor de urmărit, în dosare dedicate sau pe suport extern preautorizat;
- Accesați rețeaua numai în prezența și autorizarea prealabilă a profesorului responsabil de activitate;
- Utilizați echipamentul GPPO1 doar în scopuri educaționale și non-personale;
- Lăsați neschimbată configurația sistemului a dispozitivelor;
- Închideți-vă ședința de lucru corect. Există excepții de la utilizarea dispozitivelor de către prescolarii cu bes, pentru care este posibil să utilizeze pc-ul personal și înregistrarea lecțiilor, reglementate de eip-urile și pdp-urile respective și de legislația în vigoare. Mai mult, pentru activitățile specifice de predare organizate de profesorul clasei, utilizarea dispozitivelor personale (byod) este permisă la școală. În toate activitățile educaționale care implică utilizarea noilor tehnologii și a dispozitivelor personale, atât la școală, cât și în timpul călătoriilor educaționale, se aplică măsurile de mai sus. Părinți părinții au obligația:
- Să citească, să înțeleagă și să promoveze politica de securitate electronică cu copiii lor;
- Verifică periodic registrul electronic și site-ul instituțional al GPPO1;
- Monitorizează modul în care copiii folosesc tehnologia și îi îndrumă către un comportament responsabil și sigur;
- Colaborează cu școala pentru a desfășura activități și proiecte care implică utilizarea dispozitivelor personale (byod);
- Se confruntă cu profesorii și / sau directorul școlar al GPPO1 dacă există probleme cu privire la utilizarea noilor tehnologii de către copil.
- Instalați și utilizați doar software autorizat;
- Lăsați neschimbate setările dispozitivelor școlare;
- Completați registrul de utilizare pentru a asigura trasabilitatea activităților și întreținerea în stare bună a echipamentului tehnologic utilizat, raportând prompt managerilor orice defecțiuni, conform procedurilor prevăzute;
- Nu salvați fișierele care conțin date personale și / sau date sensibile pe dispozitivele utilizate; • nu memorați acreditările, e-mailurile, fișierele personale pe dispozitive;
- Asigurați-vă că v-ați deconectat de la fiecare serviciu înainte de a părăsi stația;
- Salvați fișierele de lucru în dosarele personale sau de clasă și nu pe desktop; fișierele care nu sunt salvate în acest mod vor fi șterse de către managerul de echipamente;
- Să folosească laboratorul care așteaptă la ora convenită la începutul anului, să semneze registrul de acces completând câmpurile necesare, să raporteze orice defecțiuni constatate înainte, în timpul sau la sfârșitul activității desfășurate;
- Să permită accesul studenților la atelier doar dacă este însoțit de profesori;
- Înainte de a părăsi laboratorul, asigurați-vă că toate calculatoarele au fost oprite corect; dacă este necesar, completați formularul pentru raportarea problemelor;
- Verificați utilizarea corectă a laboratorului și a instrumentației, asigurându-vă că nu sunt introduse alimente sau băuturi;
- Aplicați aceleași precauții în sălile de clasă amplificate de tehnologie;
- Le explică studenților acest document și le informează cu privire la orice sancțiuni disciplinare prevăzute de reglementările GPPO1;

- Asigurați-vă că accesul studenților la rețea este întotdeauna supravegheat, informați-i despre riscurile la care pot fi expuși și utilizarea corectă a rețelei (motoare de căutare, platforme online, clase virtuale);
- Previzualizați site-urile care vor fi propuse în avans, verificând cu atenție siguranța și respectarea drepturilor de proprietate intelectuală;
- Îndrumă prescolarii în cercetarea online: oferă obiective clare, propune adrese web, cuvinte cheie pentru cercetare, preferă site-urile instituționale, create special pentru predare; să urmăriți, în timpul navigării, că toată lumea folosește corect Net, oferind indicații constante cu privire la ceea ce este necesar de netiquette;
- Raportează managerilor utilizarea site-urilor de internet care nu sunt compatibile cu politica educațională a GPPO1.

PRESCOLARI

În timpul activității de predare, prescolarii trebuie:

- Accesați laboratorul informatic numai dacă este însoțit de profesori și urmați instrucțiunile furnizate privind utilizarea tic;
- Să acceseze mediile de lucru cu propriile lor credențiale, fără să le divulgă și să stocheze fișierele lor într-o manieră ordonată, astfel încât să fie ușor de urmărit, în dosare dedicate sau pe suport extern preautorizat;
- Accesați rețeaua numai în prezența și autorizarea prealabilă a profesorului responsabil de activitate;
- Utilizați echipamentul GPPO1 doar în scopuri educaționale și non-personale;
- Lăsați neschimbată configurația sistemului a dispozitivelor;
- Închideți-vă ședința de lucru corect. Există excepții de la utilizarea dispozitivelor de către studenții cu bes, pentru care este posibil să utilizeze pc-ul personal și înregistrarea lecțiilor, reglementate de eip-urile și pdp-urile respective și de legislația în vigoare. Mai mult, pentru activitățile specifice de predare organizate de profesorul clasei, utilizarea dispozitivelor personale (BYOD) este permisă la școală. În toate activitățile educaționale care implică utilizarea noilor tehnologii și a dispozitivelor personale, atât la școală, cât și în timpul călătoriilor educaționale, se aplică măsurile de mai sus.

PĂRINȚI

Părinții au obligația:

- Să citească, să înțeleagă și să promoveze politica de securitate electronică cu copiii lor;
- Verifică periodic registrul electronic și site-ul instituțional al GPPO1ui;
- Monitorizează modul în care copiii folosesc tehnologia și îi îndrumă către un comportament responsabil și sigur;
- Colaborează cu școala pentru a desfășura activități și proiecte care implică utilizarea dispozitivelor personale (BYOD);
- Se confruntă cu profesorii și / sau directorul școlar al GPPO1 dacă există probleme cu privire la utilizarea noilor tehnologii de către copil

ALTE TIPURI DE TIC

Prescolarul nu este capabil să-și folosească cunoștințele și informațiile conexe; orice utilizare în timpul unei activități didactice specifice, trebuie să fie autorizată și supravegheată constant de profesorul clasei. În orele școlare, prescolarii nu au voie să utilizeze telefonie mobilă. Infracțiunile și cele relative sunt o utilizare necorespunzătoare a TIC de către studenți sunt refuzate în Regulamentul GPPO1.

NETIQUETTE

Oricine folosește TIC, internet și serviciile oferite de Internet trebuie să respecte o serie de reguli care reglementează comportamentul utilizatorilor în relația cu ceilalți. Aceste reguli constituie așa-numita netiquette, un fel de etichetă a rețelei. Unele dintre regulile asupra cărora se dorește sensibilizarea utilizatorului sunt raportate:

- În rețea, comunicarea are loc în principal prin intermediul textelor, cu riscul consecințelor de a fi înțeles greșit; uneori, în setări adecvate, emoticoanele pot ajuta și la clarificarea tonului mesajului;
- Evitați să trimiteți mesaje repetitive, inutile sau inadecvate (spam); evita, de asemenea, trimiterea de mesaje publicitare, lanțuri sau comunicații care nu sunt solicitate în mod expres;
- Pe internet îți poți exprima opinia și ideile, respectând întotdeauna toți interlocutorii și utilizatorii mesajului; Rețeaua oferă posibilitatea de a intra în contact cu milioane de utilizatori, a căror naționalitate, cultură, religie și sex trebuie respectate; nu sunt permise forme de insultă, amenințare, rasism sau discriminare;
- Este necesar să se respecte interlocutorii virtuali: timpul lor în răspuns, care nu va fi niciodată necesar, interesul lor sau nu față de ceea ce se propune; Erorile de dactilografiere, de gramatică sau de sintaxă nu trebuie stigmatizate, important este ca transmiterea mesajului să aibă succes; Amintiți-vă că scrierea cu majuscule este echivalentă cu strigătele: nu abuzați de ea;
- Alegeți forum, social, comunitate, chat, listă de corespondență ... La care intenționați să participați pe baza subiectelor care interesează sau a nevoilor care au apărut; participa respectând regulile și intervențiile moderatorilor;
- Exprimarea opiniei cuiva trebuie să aibă loc într-un mod calm, pentru a nu provoca reacții dure la persoanele cu care se comunică;
- Să nu-și folosească abilitățile digitale pentru a încălca site-urile sau profilurile altor utilizatori, publicarea de conținut sau conversații private, partajarea de fotografii, videoclipuri sau alte fișiere ale utilizatorilor terților fără acordul lor;
- Aveți grijă de reputația dvs. Digitală, evaluând întotdeauna cu atenție ceea ce doriți să comunicați, publicați și distribuiți;
- Respectați confidențialitatea celorlalți utilizatori: fiecare poate alege ce să publice și ce să partajeze informații despre el;
- Evitați dezvăluirea de detalii, informații personale sau date personale ale altora sau ale altora;
- Utilizați Internetul în mod critic: evitați să credeți în tot ceea ce se spune și să vă feriți de cei care solicită informații personale sau întâlniri după un timp scurt în care ați intrat în contact, deoarece nu este întotdeauna posibil să aveți certitudinea identității persoanei cu care unul comunică.

CONTACTE ȘI RELAŢII ȘCOALA-FAMILIE

GPPO1 se angajează să promoveze o comunicare clară și explicită cu personalul, familiile și comunitatea, în special prin:

- Site-ul instituțional, actualizat constant, care oferă informații precise și transparente privind documentația și activitățile legate de școală;
- Registrul electronic, actualizat constant de profesori, pe care familiile pot verifica absențele, voturile și adnotările;
- Poștă electronică instituțională, un canal preferențial pentru transmiterea informațiilor și comunicării între utilizatori. GPPO1 oferă asistență familiilor pentru înregistrări online la diferite comenzi școlare prin intermediul unor posturi de calcul dedicate și personal secretar. GPPO1, ca urmare a dematerializării, are în vedere să aibă un sistem de semnături metrice grafice, conceput pentru toți utilizatorii.

Protecţia datelor sensibile în GPPO1

Datele sensibile din cadrul unei şcoli includ detaliile confidenţiale ale elevilor, părinţilor şi membrilor personalului, informaţiile şcolare, de sănătate şi psihologice ale elevilor, salariile profesorilor şi CV-urile acestora, precum şi date privind administrarea şcolii. Aceste informaţii pot fi stocate pe computerele locale, pe dispozitive mobile, pe servere localizate pe teritoriul şcolii sau în alte locaţii sau pe documente printate pe o imprimantă confidenţială sau comună. Protecţia insuficientă sau dezvăluirea improprie a acestor date poate rezulta într-o încălcare a confidenţialităţii sau a legilor de protecţie a datelor.

Ghid

Menţineţi două rețele separate de computere, unul destinat elevilor, personalului și părinţilor, iar celălalt, pe un server de înaltă securitate, destinat treburilor administrative.
Actualizaţi sistemele de protecție antivirus pentru a evita să deveniţi o țintă a hackerilor.
Criptarea și parola-proteja datele sensibile, și nu stocarea datelor ONU-criptate pe un dispozitiv portabil.
Furnizaţi personalului o formare de bază privind protejarea datelor sensibile; contactați Biroul Național pentru protecția datelor în vederea oferirii de sprijin în formare.
Creați un protocol care să fie aplicat cu rigurozitate pentru copierea sau descărcarea datelor sensibile din sistemele administrative și pentru evitarea acestui lucru ori de câte ori este posibil.
Inginerie socială [1] reprezintă cel mai mare risc de securitate; discutați cu personalul dumneavoastră pentru a vă asigura că aceştia nu se lasă păcăliţi în oferirea de date.
Nu lăsați documente ce conţin date sensibile pe imprimanta publică! Distrugeţi astfel de documente înainte să le puneţi în coșul de gunoi.
Colectaţi date sensibile doar dacă este necesar. Ceea ce nu deţii, nu poate fi compromis!

[1] Ingineria socială se referă la comunicări (prin intermediul site-urilor sau emailurilor) care păcălesc utilizatorul să viziteze un site web sau să execute click pe o legătură pentru a deschide un ataşament care oferă acces la informaţii confidenţiale.

ACŢIUNEA ŞI INTERVENŢIA PROFESORILOR

GPPO1, așa cum este evidențiat în Planul de patru ani al ofertei educaționale, acordă o atenție deosebită dezvoltării competenței digitale a prescolarilor săi, în conformitate cu prevederile Planului național pentru școala digitală (PNSD). Această competență nu poate fi separată de cele sociale și civice, mai ales pentru aspectele relaționale implicate de acestea. În acest fel, ne propunem să prevenim orice fenomen de disconfort minor. Competența digitală constă în a ști să folosești tehnologiile societății informaționale pentru muncă, timp liber și comunicare cu încredere și spirit critic. Este susținut de abilități TIC de bază: utilizarea calculatoarelor pentru a găsi, evalua, stoca, produce, prezenta și schimba informații, precum și pentru a comunica și participa la rețele de colaborare prin internet. Accentul se concentrează pe capacitatea de a explora și de a trata noile situații tehnologice într-un mod flexibil, adaptând performanța la diferitele contexte în care operează, astfel încât să analizeze și evalueze critic datele și informațiile cu care comparăm în timpul navigării online și utilizarea TIC;

- Exploatați potențialul oferit de TIC pentru rezolvarea problemelor;
- Construiește și împărtășește cunoștințele dobândite, dezvoltând o responsabilitate conștientă cu privire la datele cu caracter personal și protecția vieții private, cu o atenție deosebită asupra drepturilor și obligațiilor utilizatorilor.
- Competența digitală este interacțiunea dintre etică, inerentă responsabilității sociale, de a ști să relaționeze cu ceilalți utilizatori, de a se comporta corespunzător circumstanțelor în care se poate întâlni și de protecția propriei persoane, pentru a păstra care trebuie să știe să protejeze pe sine de eventuale riscuri;
- Tehnologie, fiind capabil să identifice utilizările și punctele tari ale dispozitivelor utilizate și, prin urmare, să aleagă dispozitivele și mijloacele adecvate pentru rezolvarea problemelor;
- Cunoștințe, datorită cărora este posibil să știi să citești, să selectezi și să evaluezi date, prin modele abstracte care duc la o analiză critică a acestora. Mass-media este văzută ca un sprijin fundamental pentru învățarea disciplinară eficientă. Profesorii au sarcina de a promova reflecția critică și experimentarea creativă, aprofundarea dinamicii care guvernează sistemul mass-media în sine, decodarea mesajelor și cunoașterea limbilor și a noilor metode și strategii de predare. GPPO1, în conformitate cu prevederile PNSD, activează cursuri de instruire pentru profesori pentru a-și spori abilitățile digitale.

PREVENTIA, DETECTAREA ŞI GESTIONAREA CAZULUI

PREVENTIA

GPPO1 își propune să ofere utilizatorilor abilitățile necesare pentru a deține un comportament responsabil și corect pentru o utilizare corectă și responsabilă în utilizarea TIC și pe net. De asemenea, este esențial să se răspândească noțiunile pentru navigare sigură, corectă și responsabilă, așa cum s-a indicat anterior în paragraful „Strategii ale GPPO1 pentru a asigura securitatea TIC”

Detectarea și gestionarea cazurilor GPPO1 se angajează să instruiască și să actualizeze cadrele didactice cu privire la modalitățile, la indicatorii pentru a recunoaște posibilele cazuri de intimidare cibernetică sau situații în pericol și procedurile care trebuie urmate. Pentru cazurile de intimidare sau intimidare cibernetică, GPPO1

lucrează pentru a proteja copiii implicați, fără a-i face identificați în vreun fel, cu date sau alte instrumente. Oricine intră în posesia anumitor date are posibilitatea de a le raporta într-o formă protejată. Când sunteți la curent cu situațiile de intimidare cibernetică:
Profesorul îl informează imediat pe .....;
Profesorul întocmește un raport asupra incidentului;
În calitate de cadru didactic, apelează separat familiile prescolarilor implicați pentru a le informa despre incident și pune în practică procedurile stabilite prin Regulamentul GPPO1. Nu uitați că, dacă este necesar, puteți contacta serviciile de asistență special active la nivel național, ORA DE NET.

Politica de Utilizare Acceptabilă a TIC de către personal 2024/2025

Utilizarea TIC în concordanță cu etosul GPPO1, cu alte politici și cu legea

Fiind vorba de o organizație profesională responsabilă cu protejarea copiilor, este important ca întregul personal să ia toate măsurile posibile și necesare pentru a proteja sistemele de date și informații împotriva infectării, accesului neautorizat, pagubelor, pierderilor, abuzului și furtului. Toți membrii personalului au responsabilitatea de a utiliza sistemul informatic al GPPO1 în mod profesional, legal și etic. Mai mult, politica BOYD *Bring your own device* (aducerea propriului dispozitiv de acasă) este adoptată astăzi în multe școli, ceea ce face ca problemele de protecție și de securitate să fie și mai dificile. Pentru a garanta că sunt pe deplin conștienți de responsabilitățile lor profesionale atunci când folosesc Tehnologiile Informaţionale şi de Comunicare membrii personalului sunt rugați să citească și să semneze Politica de Utilizare Acceptabilă.

Această listă nu este una exhaustivă și tuturor membrilor personalului li se reamintește că utilizarea TIC trebuie să fie în concordanță cu etosul GPPO1, cu alte politici adecvate și cu legea.

1. Înțeleg că Sistemele de Informații și TIC includ rețele, date și stocare de date, tehnologii de comunicare online și offline și dispozitive de acces. Exemplele includ telefoane mobile, PDA-uri, camere digitale, e-mail şi site-uri de socializare.
2. Sistemele de informare deținute de școli trebuie să fie utilizate în mod corespunzător. Înţeleg că următoarele infracţiuni pot să contravină legislaţiei în vigoare: obţinerea accesului neautorizat la date informatice; obţinerea accesului neautorizat la date informatice cu intenția de a comite sau facilita comiterea altor infracțiuni sau de a modifica datele informatice fără autorizare.
3. Înțeleg că orice material hardware și software furnizat de locul meu de muncă pentru uzul personalului poate fi utilizat doar de către membrii personalului și doar în scopuri educaționale. Pentru a preveni accesul neautorizat la sisteme sau date cu caracter personal, nu voi lăsa niciun sistem informaţional nesupravegheat fără să mă deconectez în prealabil sau fără să blochez accesul în mod corespunzător.
4. Voi respecta securitatea sistemului și nu voi dezvălui nicio parolă sau informații de securitate. Voi folosi o parola "puternică" (o parolă puternică conţine numere, litere și simboluri, este formată din 8 sau mai multe caractere, nu conține cuvinte din dicționar și este folosită doar pe un singur sistem).

5. Nu voi încerca să instalez niciun program software achiziționat sau descărcat, inclusiv toolbar-uri sau hardware fără permisiunea managerului de sistem.
6. Mă voi asigura că toate datele cu caracter personal ale prescolarilor, personalului sau părinților/tutorilor sunt păstrate în conformitate cu Legea nr. 677/2001 pentru protectia persoanelor cu privire la prelucrarea datelor cu caracter personal si libera circulatie a acestor date.
7. Aceasta înseamnă că toate datele cu caracter personal vor fi obținute și prelucrate în mod corect și legal și vor fi păstrate în confidenţialitate şi siguranță, prin intermediul unor măsuri de securitate adecvate, fie că sunt utilizate la locul de muncă, stocate online (numai în țări sau pe site-uri cu metode adecvate de control al protecției datelor) sau accesate de la distanță. Orice date preluate de pe site-ul GPPO1 (cum ar fi prin e-mail sau pe memory stick-uri sau CD-uri) vor fi criptate printr-o metodă aprobată de către școală. Orice imagini sau clipuri video ale prescolarilor vor fi folosite numai în concordanţă cu politica şcolii de utilizarea a imaginii și se va lua întotdeauna în considerare consimțământul părinților.
8. Nu voi păstra documente profesionale ce conțin informații sensibile sau cu caracter personal legate de școală (inclusiv imagini, fișiere video etc.) pe orice dispozitive personale (cum ar fi laptop-uri, camere digitale, telefoane mobile), cu excepția cazului în care acestea sunt securizate și criptate. Acolo unde este posibil, voi folosi Platforma de Învățare a Şcolii pentru a încărca documente de lucru și fișiere într-un mediu protejat cu parolă. Voi proteja dispozitivele aflate în grija mea împotriva accesului neautorizat sau furtului.
9. Nu voi utiliza sistemul informatic al GPPO1 pentru a stoca informații personale fără legătură cu activitățile școlare, cum ar fi fotografii personale, fișiere sau informații financiare.
10. Voi respecta drepturile de proprietate intelectuală și drepturile de autor.
11. Am citit și am înțeles politica de eSafetya a şcolii ce cuprinde cerințele de utilizare în condiții de siguranță a TIC, inclusiv utilizarea dispozitivelor adecvate, utilizarea în condiții de siguranță a site-urilor de socializare, precum și supravegherea prescolarilor în clasă și în alte spații de lucru
12. Voi raporta coordonatorului eSafety, Maria Ţuca toate incidentele îngrijorătoare cu privire la siguranță online a copiilor, cât mai curând posibil. Voi raporta orice acces accidental, primirea de materiale nepotrivite, breşe de securitate sau site-uri nepotrivite către Maria Ţuca coordonatorul eSafety sau către Cîrnu Maria persoana responsabilă cu filtrarea conţinutului, cât mai curând posibil.
13. Nu voi încerca să ocolesc filtrele și/sau sistemele de securitate implementate de către gradiniță. Dacă suspectez că un calculator sau un sistem a fost deteriorat sau infectat cu un virus sau cu alte tipuri de malware sau dacă am pierdut documente sau fișiere legate de școală, voi raporta acest lucru Furnizorului/Echipei de Suport TIC, cât mai curând posibil.
14. Comunicarea electronică cu, părinții/tutorii și alți profesioniști se va desfășura numai prin intermediul canalelor de comunicare aprobate de școală. Orice relații pre-existente ce ar putea compromite acest lucru vor fi discutate cu Director Prof. Cîrnu Maria, prof, Maria Ţuca si prof. Câruntu Narcisa.
15. Utilizarea TIC și a sistemelor informatice va fi întotdeauna compatibilă cu rolul meu profesional,fie că utilizez sisteme personale sau sistemele GPPO1. Aceasta include utilizarea e-mailului,mesajelor text, social media, rețele de socializare, jocuri, publicații web, precum și orice alte dispozitive sau website-uri.

Utilizarea TIC nu va interfera cu sarcinile de muncă și va fi în conformitate cu Politica de Utilizare Acceptabilă a şcolii și cu legea. Nu mă voi împrieteni cu prescolarii pe site-uri de socializare de tip Facebook.

16. Nu voi crea, transmite, afișa, publica sau trimite mai departe orice material ce poate harţui, ofensa, deranja sau cauza anxietăţi inutile oricărei alte persoane, sau orice material care ar putea compromite rolul meu profesional, școala sau .....
17. Voi promova eSafety în rândul prescolarilor aflaţi sub supravegherea mea și îi voi ajuta să dezvolte o atitudine responsabilă vizavi de siguranța online, utilizarea sistemului și conținutul pe care îl accesează sau îl creează.
18. Dacă am nelămuriri sau întrebări cu privire la siguranță și practica profesională online, fie în școală, fie în afara şcolii, le voi aduce la cunoştinţa Coordonatorului eSafety Maria Ţuca sau a directorului GPPO1.
19. Înțeleg că utilizarea sistemelor informatice, a Internetului și e-mailului poate fi monitorizată și înregistrată în vederea asigurării respectării politicii.

Şcoala îşi poate exercita dreptul de a monitoriza utilizarea sistemelor informatice, inclusiv accesul la Internet şi interceptarea de e-mail-uri, în scopul monitorizării respectării Politicii de Utilizare Acceptabilă şi Politiciide Securitate a Datelor. În cazul în care se consideră că are loc folosirea neautorizată şi/sau necorespunzătoare a sistemului informatic al serviciului sau un comportament inacceptabil sau necorespunzător, şcoala va invoca procedura sa disciplinară. Dacă şcoala suspectează că sistemul poate fi folosit în scopuri criminale sau pentru depozitarea ilegală de text, imagini sau sunet, chestiunea va fi adusă în atenția organelor responsabile cu aplicarea legii.

Am citit şi înţeles şi sunt de acord cu respectarea Politicii de Utilizare Acceptabilă a TIC de către personal.

Semnătură: …… Nume: …… Dată: …….....
Acceptat de: ..…….. Nume: …….....

PLANUL DE ACŢIUNE ESAFETY AL GPPO1

INFRASTRUCTURĂ

Securitate tehnică

Toate computerele importante ale scolii sunt protejate împotriva virusilor. Ne-am asigurat sa includem un paragraf privind protecţia antivirus în Politica scolii si în Politica de Utilizare Acceptabila, si ne-am asigurat ca personalul si prescolarii aplica în mod riguros îndrumarile scolii.

Avem un grad moderat de filtrare în scoala noastra. Luam în considerare, unde este necesar, o filtrare diferenţiata în funcţie de vârsta si nevoile diferitilor elevi. În cazul în care exista o mulţime de cazuri de utilizatori care acceseaza conţinut inadecvat, atunci se poate lua în considerare o filtrare aditionala sau educaţie suplimentara (sau ambele). O abordarea educaţionala si cresterea încrederii prescolarilor de toate vârstele sunt esentiale pentru utilizarea mediului online în condiţii de siguranţa si responsabilitate, astfel este recomandat sa reuniti toate cadrele didactice pentru o discuţie privind modul în care trebuie sa discute cu prescolarii lor despre cum sa fii un bun cetaţean digital bun.

Accesul prescolarilor şi profesorilor la tehnologie

Tuturor membrilor personalului si prescolarilor li se permite să folosească stick-uri USB de memorie în scoala. Aceasta este o practică bună si Politica de Utilizare Acceptabilă stipulezeaza că toate mediile amovibile trebuie verificate înainte de a fi utilizate în sistemele şcolii. Se consulta fisa informativă pe Utilizarea dispozitivelor mobile la pentru a ne asigura că acoperim toate aspectele legate de securitate. Deoarece personalul si prescolarii pot folosi propriul echipament în reteaua scolară, este important să ne asiguram că Politica de Utilizare Acceptabilă este revizuită în mod regulat de către toti membrii scolii si adaptată, dacă este necesar. Se discuta cu prescolarii la începutul anului şcolar, astfel încât aceştia să înteleagă regulile care le protejează confidenţialitatea şi motivele pentru care acestea sunt instituite. Ne bazam politica în jurul comportamentului, mai degrabă decât pe tehnologie. Vizitatorii trebuie să citească si să semneze Politica de Utilizare Acceptabilă înainte de a folosi reteaua scolii.

Protecţia datelor

Avem o politică bună de gestionare separată a mediilor de învătare si de administrare. Instruirea personalului este actualizată în vederea gestionării acestor medii, pe măsură ce ne revizuim politicile. Împărtăsim politica cu alţi utilizatori eSafety Label prin încărcarea ei pe profilul scolii.

Noii utilizatori primesc o parolă standard si li se cere să-şi genereze propria parolă la primul acces. Parolele oferă puncte unice de acces în sistemul informatic al şcolii si de aceea trebuie respectate riguros câteva reguli de bază privind securitatea parolei. Includem aceste reguli în Acordul cu utilizatorul şi evitam să acordam noilor utilizatori parole standard de prim acces.

Licenţe software

Ne asiguram că toti noii angajatii sunt informati în legătură cu procedurile necesare instalării de software nou. Acest lucru va însemna că securitatea sistemelor poate fi mentinută si că personalul poate încerca noi aplicatii software, lucru care va ajuta la predare si învătare.

Şcoala noastră a stabilit un buget realist pentru programele de software. Ne-am asiguram că va rămâne asa. Putem de asemenea, să căutati alternative. Spre exemplu. Servicii de cloud sau software gratuity (open-source).

Management IT

Este o bună practică să ne asiguram că persoana responsabilă cu TIC este pe deplin informată cu privire la programele instalate pe calculatoatrele şcolii. Acest lucru este indicat în mod clar în Politica scolii si în Politica de Utilizare Acceptabilă. Persoana responsabilă cu reţeaua este în măsură să garanteze conformitatea cu cerintele de licentiere si, de asemenea, că noul software nu va interfera cu functionarea retelei.
O dată pe an se iau deciziile privind achizitionarea de hardware/software nou. Găsitm metode de a permite cererilor de achizitionare hardware/software să fie făcute si pe parcursul anului. Acest lucru va permite profesorilor să creeze lectii interactive fără tentatia de a folosi materiale aflate sub incidenta drepturilor de autor.

POLITICĂ

Politica de Utilizare Acceptabilă (PUA)

Avem o Politică de Utilizare Acceptabilă pentru toti membrii comunităţii scolare. Revizuim în mod regulat PUA pentru a ne asigura că aceasta este încă adaptată scopului.
Schimbările sunt incluse imediat în politicile scolii. Luam în considerare că si schimbările din afara scolii, precum noi legislatii sau tehnologii, pot afecta politicile. Din acest motiv, ne revizuim politicile anual.

Raportarea şi abordarea incidentelor

Tot personalul este familiarizat cu procedura de gestionare a materialelor potenţial ilegale. Există o persoană desemnată din echipa de conducere a scolii care îsi asumă întreaga responsabilitate în acest caz. Procedura este comunicată în mod clar către întregul personal prin Politica scolii si către profesori si elevi prin Politica de Utilizare Acceptabilă. Raportam orice coninut suspect ilegal pe site-ul dvs. national INHOPE Hotline
Înregistrarea centralizată a incidentelor cyberbullying care au loc în scoală reprezintă o bună practică. În acest fel contribuim la construirea unei baze de date cu practici de succes în gestionarea incidentelor în scolile din întreaga Europă, pe care noi. şi alţii o putem folosi în viitor. Ne asiguram că prescolarii aderă la îndrumările anti-cyberbullying din Politica de Utilizare Acceptabilă.

Politica personalului

Pe măsură ce apar noi tehnologii si practici online, granitele practicilor acceptabile sunt din ce în ce mai neclare. Acest lucru este discutat frecvent în cadrul reuniunilor personalului. Am creat un tutorial despre comportamentul profesional online al personalului si il vom încărca pe profilul şcolii dvs. prin intermediul Şcoala mea, astfel încât alte scoli să poată beneficia de buna noastra practică.
Politica de Utilizare Acceptabilă conţine îndrumări privind utilizarea telefoanelor mobile la clasă de către cadrele didactice. Am încărcat PUA pe profilul şcolii noastre deoarece reprezintă un model de bune practici ce poate fi de ajutor altor scoli care doresc obţinerea calificativului eSafety.

Comportamentul şi practica prescolarilor

Am definit standardele comunicării electronice în Politica de Utilizare Acceptabilă si acest lucru este un exemplu de bună practică. Am realizaţ un tutorial despre standardele comunicării electronice a prescolarilor si l-am încărcat pe profilul scolii noastre la Şcoala mea, permiţând şi altor şcoli să beneficieze de experiena noastră. Scoala noastra abordează în totalitate consecinele pozitive si negative ale comportamentului prescolarilor. Aceasta este o bună practică şi am împărtăsit această politică prin intermediul Şcoala mea a portalului eSafety, astfel încât să permitem şi altor şcoli să beneficieze de ea.

Prezenţa online a GPPO1

Politica GPPO1 acoperă toate domeniile cu informaţii despre Realizarea şi publicarea fotografiilor si clipurilor video la şcoală si am încărcat această sectiune a Politicii şcolii pe pagina noastra de profil prin intermediul Şcoala mea, astfel încât să poată învăta şi alte scoli această bună practică.
Este bine că prescolarii pot da feedback cu privire la prezenta scolii în mediul online. Luam în considerare crearea unui spatiu gestionat integral de elevi. Este o oportunitate grozavă de a învăta despre competente digitale si aspecte conexe. Am stabilit o retea de colegi care să ofere suport. Se consulta fisa cu informatii eSafety

PRACTICĂ

Management eSafety

Pe lângă o desemnare clară a responsabilităilor, pentru a ne asigura că totul este în regulă cu securitatea retelei si confidenţialitatea utilizatorilor, este esential ca în scoala să aibă loc audituri si controale procedurale la interval regulate. Fără acestea, scoala va deveni vulnerabilă. Desi în şcoala existe o persoană responsabilă cu problemele de eSafety, toată lumea trebuie să împartă responsabilitatea asigurării securităţii datelor sensibile utilizate în îndatoririle profesionale de zi cu zi. Chiar si personalul neimplicat direct în manipularea datelor este constient de riscuri si amenintări, precum şi de modalităţile de minimizare a problemelor. Se consulta fisa PUA pentru a ne asigura că toţi cei implicaţi încearcă să devină nişte buni cetăţeni digitali.
Ne asiguram că managerul sau membrul din echipa de conducere responsabil cu problematica eSafety beneficiază de formare periodică si, de asemenea, ne asiguram că toţi colegii sunt constienti de problemele eSafety. Implicam consiliul de conducere în elaborarea si revizuirea periodică a Politicii şcolii noastre.

eSafety în programa şcolară

eSafety face parte din programă. Ne asiguram că toti membrii personalului predau educatia eSafety în cadrul întregii programe şcolare si nu doar în timpul orelor de curs ce tratează subiecte legate de TIC.

Suntem în măsură să oferim o programă eSafety care tine pasul cu problemele emergente. Continuam să utilizaţi noi resurse în măsura în care acestea sunt disponibile. Vom încărca la profilul scolii o schită a modului în care am conceput programa şi link-uri către resursele pe care le utilizam.

Surse de sprijin

Alte servicii scolare sunt implicate în problemele eSafety (consilieri, psihologi, asistenta şcolii). Aceştia sunt invitaţi să contribuie la elaborarea şi revizuirea periodică a Politicii şcolii noastre. Am publicat pe pagina de profil a scolii de pe site-ul proiectului eSafety Label un studiu de caz cu privire la modul în care acest lucru este gestionat în scoala noastra, astfel încât ceilali să poată învăta din experienta noastra. Avem un angajat care are cunostinte de eSafety si actionează ca persoană de încredere pentru elevi.

Formarea personalului

Instruirea periodică a personalului pe problematica eSafety reprezinta un beneficiu real pentru prescolarii nostri. Tot personalul are o oarecare formare în problematica eSafety, astfel încât să fie capabili să indice prescolarilor unde să caute îndrumare şi sprijin. Școala se asigura că membrii personalului sunt informaţi în mod periodic pentru a fi conştienţi în legătură cu problemele eSafety care-i pot afecta pe ei și pe prescolarii lor.

Este un exemplu de bună practică faptul că furnizam profesorilor informatii despre tehnologiile folosite de către elevi în timpul liber. Acest lucru este important deoarece este un prim pas în face prescolarii să se deconecteze la scoală. În acelai timp, prescolarilor nu le este cerut să folosească pentru temele de acasă tehnologie care nu le este accesibilă în afara scolii (Studiu privind TIC în scoli).

Politica GPPO1 legată de utilizarea dispozitivelor/telefoanelor mobile

A devenit din ce în ce mai dificil de pus în aplicare o interdicție absolută cu privire la utilizarea telefoanelor mobile în școli, pe de-o parte deoarece acestea au devenit indispensabile în viața tinerilor, dar şi pentru că mulți părinți insistă să poată intra în orice moment în legătură cu copiii lor. Deși prezența telefoanelor mobile poate fi deranjantă și poate conduce la comportamente deranjante precum copierea şi bullyingul, ele pot, de asemenea, să ofere oportunități fără precedent atunci când sunt utilizate în mod proactiv şi creativ în sala de clasă, atâta timp cât există o politică strictă privind deținerea și utilizarea acestora.

Politica eSafety conține instrucțiuni clare referitoare la posesia și utilizarea dispozitivelor mobile în GPPO1 și consecințele încălcării unei astfel de politici. PUA conține un protocol referitor la utilizarea dispozitivelor mobile în școala. Deși prezența telefoanelor mobile poate fi deranjantă și poate conduce la comportamente deranjante precum copierea şi bullyingul, ele pot, să ofere oportunități fără precedent atunci când sunt utilizate în mod proactiv şi creativ în sala de clasă, atâta timp cât există o politică strictă privind deținerea și utilizarea acestora. Pe durata orelor de curs, telefoanele mobile se păstrează în locuri special amenajate din sala de clasă, setate astfel încât să nu deranjeze procesul educativ.
Este permisă utilizarea acestora în timpul orelor de curs, numai cu acordul cadrului didactic, în situaţia folosirii lor în procesul educativ sau în situaţii de urgenţă. Prescolarilor le este permis să acceseze rețeaua Wi-Fi a GPPO1 prin intermediul telefoanelor lor mobile, dar aceasta este o rețea diferită de rețeaua securizată utilizată pentru personalul/activitatea de bază.

Profesorii, prescolarii și părinții sunt bine informați despre politica de folosire a dispozitivelor mobile la școală. Sunt organizate discuții regulate cu personalul în scopul revizuirii politicii referitoare la utilizarea telefonului mobil și pentru a discuta măsurile necesare atunci când are loc o încălcare a acestei politicii. Părinții sunt informați despre politica referitoare la utilizarea telefonului mobil, cu privire la motivele pentru care sunt luate aceste măsuri și cu privire la posibilele consecințe pe care le poate implica o încălcare a acestei politici. O procedură strictă este aplicată de către personal pentru a gestiona încălcările politicii care ține de dispozitivele mobile și confiscarea acestora. În cazul confiscării unui telefon mobil, elevul trebuie să oprească telefonul înainte de al transmite cadrului didactic, pentru a asigura protecția datelor private de pe telefon. Dacă telefonul nu este returnat la sfârșitul zilei de școală, părinții sunt informați și telefonul mobil este păstrat într-un loc sigur.

S-a instalat un sistem de protecție antivirus pe toate computerele din rețeaua școlară și s-a adoptat o practică constantă la nivel de școală în ceea ce privește protecția împotriva virușilor. Protecția antivirus este actualizată constant. Se solicita membrilor personalului și prescolarilor să scaneze toate dispozitivele detaşabile împotriva programelor malware înainte de a le utiliza și oferiți-le suficiente îndrumări pentru a efectua cu succes această procedură. Se permite utilizarea dispozitivelor mobile numai când sunt necesare în vederea îndeplinirii sarcinilor școlare. Prescolarilor și membrilor personalului nu li se permite să-şi conecteze aparatul foto sau un MP3 player-ul la un computer din reţeaua şcolii, cu excepția cazului în care trebuie să facă acest lucru în

cadrul unei sarcini specifice pe care au primit-o. Personalul evita stocarea datelor sensibile ale prescolarilor și ale altor membrii ai personalului pe dispozitive detaşabile cu excepția cazului în care acest lucru este necesar în vederea executării sarcinilor ce le revin, deoarece există întotdeauna riscul ca aceste dispozitive cu informații personale pe ele să fie furate sau pierdute.

Exista o procedură oficială de gestionare a incidentelor în cazul unor infecţii malware prin utilizarea unui dispozitiv mobil sau în cazul pierderii unui dispozitiv. Aceasta din urmă este deosebit de importantă dacă dispozitivul conține informații sensibile despre elevi sau personal. Personalul și prescolarii sunt încurajați să salveze fișiere pe dispozitivele mobile pe care le folosesc pe computerele școlii doar în scopuri educaționale. O procedură strictă este aplicată de către personal pentru a gestiona încălcările politicii care ține de dispozitivele mobile și confiscarea acestora. Personalul și prescolarii sunt informați cu privire la procedura de gestionare a incidentelor și o respect pe aceasta (dispozitiv pierdut, infectie cu malware). Proceduri de gestionare a incidentelor au fost implementate, în special în cazurile în care s-a pierdut un dispozitiv extern de stocare care conține date sensibile despre elevi.

Exista un protocol riguros aplicat atunci când este vorba despre descărcarea/trimiterea/printarea datelor sensibile. Există un protocol care este aplicat cu rigurozitate pentru copierea sau descărcarea datelor sensibile din sistemele administrative și pentru evitarea acestui lucru ori de câte ori este posibil. Exista două rețele separate de computere, unul destinat prescolarilor, personalului și părinţilor, iar celălalt, pe un server de înaltă securitate, destinat treburilor administrative. Avem o relație bună cu persoana de contact din cadrul Autorității Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal. Organizăm sesiuni de formare pentru personalul GPPO1 susținute de o persoană specializată. Organizăm de doua ori pe an întâlniri cu membrii personalului pentru a discuta despre importanța protecției datelor cu caracter personal, inclusiv riscurile care țin de inginerie socială. Este în vigoare procedura de gestionare a incidentelor. Este oferit sprijin profesional în vederea stocării și encriptării datelor.

Politica GPPO1 conține o secțiune dedicată publicării de fotografii în care apar sau sunt realizate de elevi, părinți și personal

Participarea copiilor într-un concert sau într-o piesă de teatru la școală este un moment de neuitat și un motiv de mândrie pentru părinți – este un moment pe care mulți vor dori să-l fotografieze sau să-l filmeze. Având în vedere accesul rapid de la un ecran de telefon mobil la un site de socializare, există anumite reguli pe care conducerea şi personalul şcolii ar trebui să le ia în considerare și să le comunice părinților.

Ghid

Asigurați-vă că școala dvs. are o politică clară referitoare la imagine şi fotografie indiferent dacă aceasta este sau nu o obligație legală în țara dvs.

Comunicați comunității școlare această politică alături de îndrumări practice clare și exemple ușor de înțeles.

Asigurați-vă că toți părinții/tutorii legali și/sau tinerii (în funcție de vârstă și cerințe naționale) au semnat un fomular de permisiune pentru foto/video ÎNAINTE de orice filmare sau fotografiere a elevilor.

Dacă părintele/tutorele nu-şi dă acordul, înțelegeţi posibilul disconfort al elevului respectiv și aranjați discret ca el/ea să aibă o altă ocupație în timpul procesului de filmare sau fotografiere.

Asigurați-vă că toţi membri comunității școlare înțeleg implicațiile partajării fotografiilor și conținutului video pe site-urile de socializare – nu postaţi NICIODATĂ numele complet, vârsta sau orice alte detalii personale alături de fotografia unui copil pe site-ul dvs.!

Ţineţi minte că evenimentele școlare sunt ocazii de bucurie care nu ar trebui să fie restricționate de prea multe reglementări.

Prezenţa şcolilor pe reţelele de socializare

Folosirea reţelelor de socializare de către şcoli este un subiect controversat, putând fi aduce argumente pentru şi împotrivă, de la riscul cyberbullying-ului şi prieteniile online dintre elevi şi profesori până la promovarea activă pe care o poate aduce Twitter. De la dezvoltarea profesională până la descoperirea de exemple din viaţa reală la orele de limbi străine, socializarea media în şcoli poate reprezenta o resursă valoroasă. Cel mai important lucru care trebuie avut în vedere în legătură cu utilizarea reţelelor de socializare în şcoli este chestiunea drepturilor şi responsabilităţilor online.
Pe lângă rolul de intrument promoţional pentru şcoli, profesorii din toată lumea au enumerat mai jos beneficiile utilizării reţelelor sociale în şcoli.

Ghid
Dezvoltarea profesională în ceea ce privește utilizarea instrumentelor tehnice și de social media pentru profesori.
Utilizarea unor metode de învățare moderne, incluzive și alternative.
Informarea și sensibilizarea comunităţii şi a părinților prin intermediul grupurilor de Facebook, Pinterest, Yammer, Twitter și altele.
Comunicarea cu părinții în cazul în care sunt prieteni pe Facebook cu școala/clasa/ proiectul școlar.
Comunicarea interculturală cu alte școli.
Învățarea limbilor străine.
Învățarea colaborativă și împărtăşirea de informaţii cu colegi și grupuri educaţionale cu aceleaşi interese.
Stabilirea de legături cu colegi din întreaga țară și chiar din lume.
Integrarea unor exemple din lumea reală în procesul de predare.

Practică

În această secţiune veţi găsi formulare şi liste de verificare legate de cele mai bune practici eSafety pentru o şcoală. Formularele şi listele de verificare vor servi ca ghid, oferindu-vă cunoştinţele ce vă vor permite să implementaţi procesele necesare asigurării siguranţei membrilor şcolii dumneavoastră.
De asemenea, veţi avea posibilitatea să împărtăşiţi listele de verificare şi să le oferiţi altor profesori din şcoala dumneavoastră sprijin şi îndrumări, lucrând împreună cu Comitetul eSecuritate şi managerul IT sau de reţea.

Încorporarea siguranței online în curriculum

Deşi TIC și mediul digital oferă copiilor și adolescenților un potențial enorm de a explora, de a se conecta și de a crea, elevii au nevoie de îndrumări suplimentare cu privire la comportamentul sigur și responsabil în mediul online. În special, ei trebuie să învețe strategii eficiente de găsire a unui echilibru între oportunități și riscuri, de gestionare a informațiilor online și a securității acestora, de protejare a intimităţii lor și respectare a celuilalt, de gestionare a cazurilor de cyberbullying, de a distinge între contacte şi conţinut nepotrivit și pozitiv, ș.a.m.d.

Ghid
Asigurați-vă că eSafety se predă ca parte a programei, indiferent dacă aceasta este sau nu o obligație legală în țara dvs.
Deşi predarea eSafety în cadrul cursurilor de TIC sau media pare cea mai potrivită abordare, școala ar trebui să urmărească o abordare trans-curriculară mai cuprinzătoare, care explorează numeroasele legături dintre eSafety și toate tipurile de conținut educațional.
Deoarece eSafety reprezintă o responsabilitate trans-curriculară, toate cadrele didactice ar trebui să beneficieze de formare periodică pe teme cum ar fi: confidenţialitatea și securitatea, amprenta digitală și reputația, cyberbullying-ul, alfabetizarea informațională etc.
În predarea acestora și altor probleme eSafety încercați să porniți de la ceea ce elevii știu deja și de la felul în care experimentează ei mediul online.
Încurajaţi elevii să se implice în mentorat la egal la egal și facilitaţi discuții interactive de jos în sus.

Sugestii pentru cursuri online de instruire în siguranță

Cercetările au constatat ca unul dintre domeniile-cheie ale eSafety care lipsește în multe școli este formarea şi conştientizarea personalului 360 degree safe self review tool.
Școlile trebuie să se asigure că membrii personalului sunt informaţi în mod periodic pentru a fi conştienţi în legătură cu problemele eSafety care-i pot afecta pe ei și pe elevii lor.

Ghid
Principii generale de formare eSafety
eSafety acoperă o gamă largă de probleme și nu trebuie abordată izolat.
Tot personalul trebuie să aibă o oarecare formare în problematica eSafety, aşa încât să fie cel puţin capabili să indice elevilor unde să caute îndrumare şi sprijin.
Personalul trebuie să fie informat cel puțin o dată pe an, pentru a se putea ține cont de schimbările survenite în obiceiurile tinerilor și în tehnologiile și aplicațiile pe care aceştia le folosesc.
În vederea eficientizării formării poate fi utilă o evaluare a nevoilor de formare a personalului şcolii.
Şcolile pot dori să ia în considerare utilitatea desemnării unei persoane responsabile cu coordonarea eSafety, însă ar trebui să fie clar că eSafety este responsabilitatea fiecărui membru al personalului.

Informații pentru părinți

Părinții joacă un rol vital în siguranța online a copiilor și tinerilor. Desigur, școlile sunt în măsură să adopte multe măsuri, pot filtra, monitoriza și educa, dar trebuie să recunoaștem că mulți copii și tineri vor avea acasă sau prin intermediul unui dispozitiv mobil un nivel foarte diferit de acces la Internet decât la școală. Mulţi părinţi sunt destul de eficienţi în îngrijirea și îndrumarea copiilor cu privire la problemele offline, dar sunt reticenţi în încercarea de a le oferi sprijin similar în ceea ce priveşte aspectele digitale ale vieții lor. Parţial acest lucru poate fi un rezultat al faptului că mulți părinți spun despre copiii lor că "se pricep mai bine la tehnologie" decât ei.

Ghid

Școlile trebuie să ofere sprijin, îndrumare și consiliere pentru părinți. Acest lucru poate lua diverse forme, o discuţie specifică pe această temă, pliante despre diferite probleme, legături (link-uri) pe site-ul școlii sau un articol în buletinul online al școlii.

Este important să recunoaștem că de multe ori părinții care participă la o seară eSafety sunt tocmai părinții care probabil nu au nevoie să participe! Părinții interesaţi de ceea ce fac copiii lor vor fi, de asemenea, mult mai conștienți cu privire la problemele cu care aceştia se confruntă online și vor fi dornici să comunice pe aceste teme.

Școlile raportează că implicarea părinţilor în problemele eSafety poate fi o provocare și că aceştia sunt de multe ori reticenţi în a veni la școală pentru astfel de evenimente. În acest caz se recomandă implicarea copiilor și tinerilor în livrarea acestor mesaje, deoarece părinții sunt mai înclinaţi să vină la un eveniment în care copilul lor participă direct, de exemplu, prin susţinerea unei prezentări. O altă strategie este livrarea mesajelor eSafety în timp ce părinții sunt deja în școală cu alte scopuri.

https://www.esafetylabel.eu/group/community/information-for-parents
Pupil's use of online technology outside school
Incident handling
Cyberbullying
Sexting
Online extremism, radicalisation and hate speech

GPPO1are o politică clară referitoare la imagine și fotografie. Toți profesorii, părinții, prescolarii și membrii comunității școlare sunt informați în mod regulat cu privire la această politică. Scopul este acela de a înţelege cât de importante sunt imaginile și clipurile video în viața digitală a prescolarilor, demonstrând rolul pozitiv pe care îl joacă acest lucru, precum și riscurile și presiunile cu care se pot confrunta ca rezultat.
Școala a comunicat comunității școlare această politică alături de îndrumări practice clare și exemple ușor de înțeles. Toți părinții/tutorii legali și/sau tinerii (în funcție de vârstă și cerințe naționale) au semnat un fomular de permisiune pentru foto/video ÎNAINTE de orice filmare sau fotografiere a prescolarilor. Dacă părintele/tutorele nu-și dă acordul, se aranjează discret ca el/ea să aibă o altă ocupaţie în timpul procesului de filmare sau fotografiere.
GPPO1 s-a asigurat că toţi membri comunității școlare înțeleg implicațiile partajării fotografiilor și conținutului video pe site-urile de socializare – nu postaţi NICIODATĂ numele complet, vârsta sau orice alte detalii personale alături de fotografia unui copil pe site-ul dvs.!
Evenimentele școlare sunt ocazii de bucurie care nu ar trebui să fie restricționate de prea multe reglementări. Orice imagini sau clipuri video ale prescolarilor vor fi folosite numai în concordanţă cu politica școlii de utilizarea a imaginii si se va lua întotdeauna în considerare consimtământul părintilor. Politica GPPO1 subliniază importanța asigurării faptului că toți copiii trebuie sa dezvolte abilitățile, cunoștințele, încrederea și reziliența de a comunica cu imagini și clipuri video în condiții de siguranță, responsabilă și creativă.
Doamna profesor, Țuca Maria este responsabil pentru verificarea că lângă pozele prescolarilor de pe website sa nu apara date personale. Gradinita păstrează o bază de date unde politica și documentele suport (acord de fotografiere/filmare) pot fi găsite cu ușurință. Toți profesorii știu la cine pot apela pentru îndrumare în cazul în care au nelămuriri. Toată comunitatea școlară, inclusiv prescolarii, au primit instruire cu privire la

producerea de fotografii și utilizarea rețelelor sociale. Un memento este trimis tuturor înainte de un eveniment școlar.

Siguranța online figurează în curriculum

eSafety se predă ca parte a programei. Există o abordare a întregii grădinițe privind siguranța online, cu un rol important al tuturor membrilor personalului, împreună cu politici de sprijin care sunt înțelese de toți cei din comunitatea școlară, pentru ca niciun copil să nu rămână vulnerabil. Politicile grădiniței se referă în mod explicit la integrarea eSafety în programă, astfel încât toți profesorii au luat la cunoștință această responsabilitate comună, pentru a înțelege de ce educația mediatică și dimensiunile sale diferite sunt importante pentru elevi, modul în care alfabetizarea media afectează unele probleme de actualitate, cum ar fi știrile false, confidențialitatea datelor și drepturile de autor. Practicile educaționale își propun să abordeze agresiunea într-un mod holistic, ajutând prescolarii să-și exercite drepturile fundamentale la domiciliu, la grădiniţa, la clasă și în comunitate, dezvoltarea abilităților sociale și emoționale de învățare ca mijloc de construire a rezistenței în rândul prescolarilor pentru ca aceștia să poată înțelege mai bine și să devină mai responsabili și mai eficace pentru interacțiunile lor sociale și online.

Protecţia datelor este inclusă în programa şcolară. Şcoala utilizeaza programe educaționale pentru elevi și personal, care variază de la prevenirea agresiunii cibernetice la protejarea identității profesionale; crearea de strategii de îmbunătățire școlară și producerea de materiale inovatoare de sprijin.

Infrastructura TIC este suficient securizată; la fiecare 90 de zile utilizatorilor li se solicită în mod automat să-şi reînnoiască parolele de acces la sistemul şcolii. Prescolarii învața strategii eficiente de găsire a unui echilibru între oportunități și riscuri, de gestionare a informațiilor online și a securităţii acestora, de protejare a intimităţii lor și respectare a celuilalt, de gestionare a cazurilor de cyberbullying, de a distinge între contacte şi conţinut nepotrivit și pozitiv. Utilizarea dispozitivelor mobile este incorporată în mod constructiv în curriculum.
Toate cadrele didactice beneficiază de formare periodică eSafety. Şcoala oferă sprijin eSafety pentru elevi în afara programei. Deşi predarea eSafety în cadrul cursurilor de TIC sau media pare cea mai potrivită abordare, școala urmăreste o abordare trans-curriculară mai cuprinzătoare, care explorează numeroasele legături dintre eSafety și toate tipurile de conținut educaţional. Deoarece eSafety reprezintă o responsabilitate trans-curriculară, toate cadrele didactice beneficieaza de formare periodică pe teme: confidenţialitatea și securitatea, amprenta digitală și reputația, cyberbullying-ul, alfabetizarea informațională, etc. În predarea acestora și altor probleme eSafety cadrele didactice pornesc de la ceea ce prescolarii știu deja și de la felul în care experimentează ei mediul online. Prescolarii sunt încurajaţi să se implice în mentorat de la egal la egal și în discuții interactive de jos în sus. Prescolarii se monitorizează reciproc pe probleme legate de eSafety.

Există oportunități de prezentare a unor contra-narative la discursul instigator la ură și extremism online prin curriculum. Radicalizarea online violentă este un proces complex prin care indivizii, prin interacțiunile lor online și expunerea la diferite tipuri de conținut pe internet, să considere violența drept o metodă legitimă de soluționare a conflictelor sociale și politice. Unii dintre cei radicalizați violent prin intermediul internetului pot continua să comită acte de terorism.
Ca răspuns la discursul de ură, educația cetățeniei cuprinde cunoștințele și abilitățile necesare pentru a identifica discursurile de ură, permițând indivizilor să contracareze mesajele de ură.

Prescolarii sunt ajutati să dezvolte abilitățile de comunicare și interpersonale de care au nevoie pentru dialog, să se confrunte cu dezacordul și să învețe abordările pașnice de schimbare.
Prescolarii sunt ajutati să-și dezvolte gândirea critică pentru a investiga revendicările, pentru a verifica zvonurile și a pune la îndoială legitimitatea și recursul credințelor extremiste. Prescolarii sunt ajutaţi să dezvolte rezistența pentru a rezista narațiunilor extremiste și pentru a dobândi abilitățile sociale și emoționale de care au nevoie pentru a-și depăși îndoielile și pentru a se angaja constructiv în societate fără a trebui să recurgă la violență. Menținerea unui dialog deschis între elev și profesor - și copilul și părintele - este una dintre cele mai eficiente modalități de a ajuta copiii și tinerii să rămână în siguranță online.
Deşi infrastructura noastră TIC este suficient de securizată, iar accesul la internet este filtrat, acest lucru nu limitează capacitatea prescolarilor noştri de a explora multitudinea de oportunităţi online.
Școala are în derulare proiecte naționale, eTwinning și Erasmus, care au la bază noile metodologii CLIL, STEM, PBL, așa că fiecare cadru didactic indiferent de vârsta elevului, de disciplina predată integrează eSafety în curriculum, fiind cea mai potrivită abordare pentru însușirea corectă a utilizării în siguranță. Integul personal al GPPO1 are integrat în programă conştientizarea cu privire la hărțuirea online, sexting, extremismul online, radicalizarea și discursul de ură, pentru toate categoriile de vârstă.

GPPO1 oferă părinților informații despre siguranța online

Educația despre siguranța online, ar trebui să înceapă cu siguranță la domiciliu, părinții jucând un rol vital în siguranța online a copiilor, dar în nici un caz nu este responsabilitatea exclusivă a părinților; profesorii trebuie să fie, de asemenea, în măsură să ofere prescolarilor lor, cu toate instrumentele necesare pentru a face față în lumea online într-o manieră puternică și responsabilă.
GPPO1 adoptă măsuri, filtreaza, monitorizeaza și educă, dar mulți copii au acasă sau prin intermediul unui dispozitiv mobil un nivel foarte diferit de acces la Internet decât la școală. În cadrul ședințelor pe școală, părinții au fost sfătuiți să monitorizeze utilizarea calculatorului, a telefonului și a Internetului de către copiii lor, acasă. Să verifice site-urile pe care le-a accesat copilul, programele și fișierele. Părinții au fost sfătuiți să restricționeze accesul la anumite site-uri pe baza unei liste predefinite de adrese interzise și să permită accesul doar la anumite site-uri pe baza unei liste predefinite de adrese acceptate.

Mulţi părinţi sunt destul de eficienţi în îngrijirea și îndrumarea copiilor cu privire la problemele offline, dar sunt reticenţi în încercarea de a le oferi sprijin similar în ceea ce priveşte aspectele digitale ale vieții lor. Școala oferă părinților sprijin, îndrumare și consiliere.

Acest lucru se realizeaza prin diverse forme, discuţii specifice pe această temă, pliante despre diferite probleme, legături (link-uri) pe site-ul GPPO1 sau un articol în buletinul online al GPPO1.

Părinții sunt rugați să-și asume un rol activ eSafety la școală și să întărească mesajele cheie. Acest lucru este subliniat în mod clar în acordul familie/școală. Sesiunile pentru părinţi legate de eSafety au loc de doua ori pe an. Mesajele privind eSafety sunt diseminate către părinţi prin intermediul unor medii diferite de comunicare. Prescolarii sunt implicaţi în transmiterea mesajelor eSafety către părinţi.
Școala le face cunoscut părinților și prescolarilor că violența online nu este tolerată în școală și sunt încurajați să semnaleze orice incident. Se verifică periodic soluțiile de securizare a rețelei informatice din școală, iar prescolarii nu sunt lăsați nesupravegheați în laboratorul de informatică.

GPPO1 foloseşte strategii de implicare a părinţilor în chestiunile legate de bullying şi cyberbullying- seri de informare, sfaturi pe site-ul şcolii. Are proceduri implementate care oferă sprijin părinţilor care întâmpină acasă dificultăţi legate de cyberbullying.
GPPO1 are strategii implementate de a discuta cu părinții despre probleme legate de extremism online și radicalizare (informații pe website, întâlniri cu părinții) și proceduri implementate care să ofere sprijin părinților care întâmpină dificultăți în a înțelege extremismul online și radicalizarea în afara GPPO1.
Părinții sunt informați și implicați în politicile care țin de utilizarea rețelelor sociale.

Personalul GPPO1 beneficiază în mod regulat de formări pe teme de siguranță online

Deoarece eSafety reprezintă o responsabilitate trans-curriculară, toate cadrele didactice beneficieaza de formare periodică pe teme: confidenţialitatea și securitatea, amprenta digitală și reputația, cyberbullying-ul, alfabetizarea informațională, eSafety acoperă o gamă largă de probleme și nu trebuie privită în mod izolat. eSafety este responsabilitatea fiecărui membru al personalului. Tot personalul are o oarecare formare în problematica eSafety, aşa încât să fie cel puţin capabili să indice prescolarilor unde să caute îndrumare şi sprijin. Personalul este informat cel puțin o dată pe an, pentru a se putea ține cont de schimbările survenite în obiceiurile tinerilor și în tehnologiile și aplicațiile pe care aceştia le folosesc. PUA este cunoscută şi înţeleasă de către toţi membrii personalului. Personalul GPPO1 pune în discuție în mod regulat siguranța pe Internet, pentru a le dezvolta prescolarilor un comportament mai responsabil când folosesc rețelele sociale sau webcam-urile, ori când transmit mesaje, colectează informații sau postează pe blog-ul personal.

Personalul este informat regulat, cel puțin anual, cu privire la problematica eSafety. Întreg personalul a beneficiat de formare eSafety în ultimele 12 luni. Există un program planificat de formare eSafety orientat spre diferite categorii de personal. eSafety face parte din instructajul introductiv oferit noilor membrii ai personalului. Formarea profesională continuă este actualizată si face referire la trenduri si aspect ce tin de eSafety. Formarea eSafety este realizată de către un trainer specializat pe domeniul siguranței online. Pregătirea personalului în domeniul eSafety este facută din trei în trei luni. Toți profesorii primesc instruire în mod regulat pe teme ce țin de eSafety și sunt implicați în formare profesională continuă. Se organizeaza anual cursuri de formare a personalului cu privire la rezolvarea mai eficientă a problemelor online. Întregul personal beneficiază de formare periodică cu privire la caracteristicile bullying-ului online şi offline, sexting, extremism online și radicalizare, metodele adecvate de răspuns în acest tip de situații și incidentele privite ca o oportunitate de a învăța.

Atelierele destinate personalului despre utilizarea rețelelor sociale sunt ținute la fiecare șase luni.

Personalul GPPO1 este informat de către doamna coordonator a comisiei eSafety, inf. Terterean Aurelia cu privire la noile reglementări care apar în decursul anului privind privind protecția datelor sensibile ale GPPO1 și a celor personale prin crearea/reînnoirea parolelor, utilizarea dispozitivelor detașabile și obligativitatea scanării fiecărui dispozitiv înaintea folosirii, utilizarea telefoanelor ținând cont de reglementările în vigoare din ROFUIP și ROI din anul în curs, procedurile de gestionare a incidentelor în cazul infectării malwere dacă este cazul pentru calculatoarele GPPO1.

GPPOstroveni 1
Oraş Râmnicu Vâlcea, Judeţ Vâlcea
Str. Aleea Teilor Nr. 5,
cod poştal 240077, tel: 0350414817
e-mail: gppostroveni1@gmail.com
Site: https://gradinitaostroveni1.ro

GPPO1 sărbătorește „Ziua siguranței pe Internet”

Celebrarea zilei Internetului a oferit posibilitatea de a evidenția utilizările pozitive ale tehnologiei și de a explora rolul pe care îl jucăm cu toții în a contribui la crearea unei comunități online mai bune și mai sigure. Sărbătorită la nivel mondial, tema siguranţei online capată valori universale, în care prescolarii se pot manifestă, pot comunica liber, pot schimbă exemple despre experienţele lor online.

Pe data de 6 februarie 2024 prescolarii din GPPO1 au accesat siteurile Web We Want, ENABLE**,** INS@FE, Google (https://pipl.com pentru a vedea cât de multe informații există online despre..).

Au vizionat videoclipuri, știri, resurse, activități, au completat o varietate de autoevaluări despre probleme precum identitate online, efectul net și reputația online, protecția datelor, confidențialitatea datelor, identificarea știrilor false, drepturile de autor, plagiatul și pirateria. Au jucat jocuri online.

Together for a better internett 2024

https://school-education.ec.europa.eu/en/etwinning/projects/every-mother-best-her-own-way/twinspace/pages/celebrating-sid

Evenimente

Eveniment de învățare 2024-2025:

Următoarea Zi a Siguranței pe Internet (SID) va avea loc în februarie 2025 cu tema "Împreună pentru un internet mai bun". O zi globală va avea loc marți, 11 februarie, cu evenimente de sărbătoare care vor avea loc pe tot globul, pe tot parcursul lunii. Prin această campanie, facem apel la toate părțile interesate să se unească pentru a face internetul un loc mai sigur și mai bun pentru toți, în special pentru copii și tineri. Un obiectiv cheie al proiectului Better Internet for Kids este de a crește gradul de conștientizare și de a împărtăși bunele practici cu privire la diferite instrumente și metode pentru a îmbunătăți experiențele online pentru copii și tineri.

Toate cadrele didactice din GPPO1 colaborează la activități eTwinning (proiecte, evenimente, promovare, dezvoltarea profesională)

eTwinning oferă un potenţial ridicat pentru cooperarea profesorilor, în egală măsură între şcoli din diferite ţări, dar şi între profesori din aceeaşi şcoală.

Profesorii de diferite discipline îi antreneaza pe elevi în diverse situaţii educative, le stimulează imaginaţia, gândirea divergentă, creativitatea. Prin lucrul în echipe, profesorii promovează interdisciplinaritatea, asigură o învăţare pe o anumită problematică, ce posedă o mare forţă formativă asupra prescolarilor. Echipa eSafety si echipa eTwinning sunt necesare în şcoala noastră pentru a garanta succesul prescolarilor în viaţă. Fără o colaborare strânsă între colegii din şcoală, este dificil să se realizeze proiecte de impact. Aceste echipe sunt conduse de un lider care împarte responsabilităţile şi monitorizează desfăşurarea proiectului. În viaţa de zi cu zi nu se pot folosi cunoştinţe disparate, de aceea este important ca profesorii să poată transmite prescolarilor legături ce definesc informaţiile, nu doar concepte abstracte.

Evenimentele de promovare eTwinning organizate în GPPO1 in care au participat și alți membri ai personalului școlii sau familiile prescolarilor

Părinții participă la activități extracurriculare, în calitate de profesioniști, reprezentanţi ai unei instituţii partenere sau ca simpli spectatori. Membri ai personalului școlii și familiile prescolarilor participă la diferite reuniuni ale prescolarilor, expoziții, cercuri metodice, reuniuni profesionale, lecții demonstrative cu activități

din proiecte, prezentări ale rezultatelor unui proiect, expunerea produselor finale ale proiectului. Membri ai personalului școlii participă la discuţii cu colegii în pauză, cu părinții și cu conducerea școlii, articole pe site-ul școlii, mese rotunde sau partajând proiecte reușite ale școlii prin social media. Părinții participă la diverse întâlniri, ateliere de lucru pentru realizarea unor afișe, pliante, bannere, materiale personalizate, articole în presa locală, buletine informative. Participă in calitate de vizitatori în TwinSpace, la anumite sondaje, instrumente de vot și la diseminările de proiecte.

Elaborat:
Prof. Țuca Maria
Director Prof. Albinaru Maria-Corina
Prof. Feloiu Ramona Georgeta
Prof. Manda Cristina
Prof. Vărgăluță Maria Mălina