



Nr. 3158/28.10.2022

Director,

Prof. Cristina DEDIU



POLITICI DE SIGURANȚĂ ONLINE ÎN UTILIZAREA PLATFORMELOR EDUCAȚIONALE ÎN ACTIVITĂȚILE ȘCOLARE ȘI EXTRAȘCOLARE ALE ȘCOLII GIMNAZIALE NR. 29 GALAȚI

Școala Gimnazială Nr. 29 Galați susține drepturile elevilor, personalului didactic, nedidactic și auxiliar didactic, de a avea acces la școală, la diferite formate de informare și este în sarcina elevilor și personalului din școală să folosească acest avantaj educațional într-un mod adecvat și responsabil.

Pentru asigurarea securității elevilor online, la nivelul unităților de învățământ sunt necesare:

- infrastructuri IT sigure, pregătite și la nivel hardware, cât și la nivelul aplicațiilor software utilizate, pentru a face față amenințărilor de securitate cibernetică din prezent;
- programe educaționale pentru elevi în domeniul securității online;
- pregătirea adecvată a personalului didactic sau existența de personal specializat în problematica siguranței online;
- părinți conștienți de existența riscurilor online și de necesitatea cooperării cu unitatea școlară pentru siguranța copiilor.

În cadrul Școlii Gimnaziale Nr. 29, Galați:

- Orele de tehnologia informației și a comunicațiilor prevăzute în curriculum se desfășoară, de regulă, în cabinetele de informatică ale școlii sub supravegherea profesorului de specialitate.





- Tot în vederea dezvoltării competențelor digitale ale elevilor și a personalului didactic, la unele ore, profesorii, împreună cu elevii, pot desfășura activitatea didactică în laboratoarele de informatică sau în cabinetele specializate, prevăzute cu calculatoare, laptopuri, videoproiectoare, tablă inteligentă, unde se pot accesa platformele educaționale indicate de profesor.

- Folosirea instrumentelor TIC permite elaborarea și implementarea metodelor moderne de predare-învățare, specifice secolului al XXI-lea. Astfel, în timpul orelor elevii au ocazia de a viziona filmulețe, prezentări power-point, documente word, pdf, imagini, care fac orele mai atractive decât mijloacele tradiționale table și manualul.

- Cabinetele de informatică/cabinetele de specialitate/laboratorul de fizică pot fi folosite de către profesori și elevi și pentru activități extrașcolare, cum sunt proiectele europene (Erasmus+, eTwinning) sau internaționale/transfrontaliere.

- În timpul accesării platformelor educaționale sau a site-urilor necesare activității, elevii vor respecta indicațiile profesorului, intrând doar pe site-urile permise, considerate sigure din punct de vedere al virușilor cibernetici.

Standardele pentru protecția și siguranța copiilor/elevilor în mediul online sunt fundamentate pe Standardele de calitate pentru instituțiile de învățământ primar și secundar general din perspectiva școlii prietenoase copilului și sunt la fel structurate pe trei domenii: Management, Capacitate instituțională, Curriculum/proces educațional. Totodată, la elaborarea Standardelor pentru protecția și siguranța copiilor/elevilor în mediul online s-a ținut cont de: – Recomandările Consiliului Europei privind promovarea educației privind cetățenia digitală, prin care într-un mod sistemic sunt dezvoltate abilități de gândire critică și competențe menite să contribuie la siguranța copiilor în mediul online⁴. – Recomandările OECD (Organizația pentru Cooperare și Dezvoltare Economică) și Cadrul European pentru competențe digitale DigCompOrg al Comisiei Europene⁵, privind abordarea comprehensivă a siguranței online de către instituțiile de învățământ, presupunând integrarea siguranței online în toate aspectele activității școlare, în toate politicile, procedurile și procesele din școală. – Planul de Acțiuni privind Educația Digitală, elaborat și aprobat de Comisia Europeană, care accentuează cât de





importantă este siguranța online și „igiena digitală” în contextul dezvoltării competențelor digitale⁶. Standardele pentru protecția și siguranța copiilor/elevilor în mediul online vin să asigure acel cadru minim necesar de acțiuni ce pot fi întreprinse de instituțiile de învățământ general pentru a-și consolida efortul în promovarea siguranței online, crearea unui mediu sigur și protejat pentru copil/elev, stabilirea măsurilor de informare cu regularitate a cadrelor didactice, părinților și copiilor/elevilor despre siguranța online.

Tehnologiile online prezintă multe posibilități de a comunica, de a învăța noi abilități, de a fi creativ și contribuie la dezvoltarea unei societăți mai bune pentru toți, dar de cele mai multe ori, de asemenea, prezintă noi riscuri: pot expune copiii și tinerii la pericole potențiale precum conținutul ilegal, viruși, hărțuire sexuală (de exemplu: în camerele de chat), utilizarea abuzivă a datelor personale sau pentru scopuri sexuale (Grooming). Nu există o soluție magică pentru a proteja copiii online. Aceasta este o problemă globală care necesită un răspuns global din partea tuturor segmentelor societății, inclusiv copiii și tinerii înșiși.

Siguranța copiilor online în instituțiile de învățământ contribuie direct la realizarea Obiectivului de dezvoltare durabilă (în continuare - ODD) nr. 4, „Educație de calitate”, și ODD 16, Ținta 16.2, „Stoparea abuzului, neglijării, exploatării, traficului și tuturor formelor de violență și tortură a copiilor”.





I.POLITICA SIGURANȚEI PE NET A ȘCOLII GIMNAZIALE NR. 29, GALAȚI

Siguranța online este parte integrantă a mai multor politici ale **Școlii Gimnaziale Nr. 29, Galați**. Aspecte privind siguranța online se regăsesc în documente cum ar fi Planul de dezvoltare instituțională, Planul managerial, Procedurile interne ale școlii, Regulamentul de ordine interioară.

Argument

Dezvoltarea rapidă a Internetului și altor tehnologii informaționale și comunicaționale a dat naștere unui flux nou și rapid de informații, produse și servicii digitale. Cu toate că această dezvoltare contribuie considerabil la modernizarea procesului educațional, și în general, la creșterea economiei naționale, ea are și o latură negativă care se manifestă prin distribuirea conținutului și comportamentelor ilegale și dăunătoare care sunt îndeosebi periculoase pentru copii și adolescenți. Copiii sunt din ce în ce mai expuși la pericolele spațiului digital, printr-o gamă tot mai mare de dispozitive care le devin accesibile de la o vârstă tot mai mică. Conceptul de siguranță online este unul relativ nou. Încă în anii anii '90, când încep să se contureze niște tendințe noi în comportamentele persoanelor care manifestă atitudini abuzive față de copii, organizații guvernamentale și neguvernamentale din Europa pun problema identificării unor soluții prin care copiii sunt protejați de astfel de tentative, dar și de impactul conținuturilor online, mai nou, atât de accesibile. Astfel, educația devine unul dintre cei mai importanți piloni în prevenirea diferitor forme de abuz online și pregătirea copiilor pentru interacțiunea cu lumea virtuală. În mai multe state europene siguranța online capătă tot mai mult o perspectivă





educațională și Comisia Europeană propune un Cadru de referință pentru Competența digitală a cetățenilor ce face referință la cinci domenii de bază ce reflectă și siguranța online. Conform Uniunii Internaționale pentru Telecomunicații (UIT), conceptul de siguranță în mediul online presupune informarea copiilor despre oportunitățile existente online, abilitarea acestora să recunoască riscurile și să identifice modalitățile prin care le pot face față, utilizând Internetul în mod sigur și responsabil. Siguranța în mediul online este o responsabilitate a fiecărui profesor din școală.

Cum realizăm Siguranța Online?

Infrastructură

Internetul aduce o gamă largă de beneficii și oportunități, dar prezintă și riscuri. Pe lângă conținutul pozitiv, există site-uri mai dificile și mai problematice, de care școlile trebuie să protejeze copiii și tinerii. *Filtrarea și monitorizarea* sunt două metode pe care școlile le pot implementa pentru a face acest lucru, dar, desigur, aceasta este o soluție parțială, iar educația este foarte importantă.

Politică

Școlile au politici pentru orice astăzi, însă aceste politici sunt eficiente numai dacă reflectă de fapt ce se întâmplă în cadrul unei școli sau al unei organizații. De asemenea, este important să recunoaștem că schimbările și politicile trebuie revizuite în mod regulat - acest lucru este valabil în special în cazul abordării siguranței online. Toate părțile interesate (elevii, personalul și părinții) ar trebui să fie implicați în crearea și actualizarea unor astfel de politici pentru ca acestea să fie eficiente și într-adevăr să contribuie la crearea și susținerea unui mediu sigur pentru elevi și personal.





Practică

Chiar și cea mai bună filtrare din lume nu este suficientă pentru a proteja copiii și tinerii atunci când merg online. De exemplu, sute de ore de videoclipuri sunt încărcate pe YouTube în fiecare minut, de aceea alături de filtrare și monitorizare, *este nevoie de educație*. Atunci când ceva se întâmplă, elevii știu ce să facă? Sunt conștienți de modul în care să raporteze ceva - nu doar unui profesor sau părinților, ci și proprietarului site-ului pe care îl utilizează? *Educația este esențială* și trebuie să fie adecvată vârstei, progresivă și încorporată în curriculum. Siguranța online nu poate fi văzută ca o anexă și nu poate fi predată în mod eficient ca un ansamblu unic sau "zi de siguranță online".

Responsabilități

Comisia pentru siguranța în mediul online este coordonată de directorul adjunct profesor Țurcanu Geanina. Acesta se ocupă de implementarea și monitorizarea politicii siguranței pe net a școlii, raportând după caz directorului Dediu Cristina, diriginților sau profesorilor orice schimbare importantă în utilizarea tehnologiei sau dacă este cazul discută evenimente care se petrec în școală privind acest aspect.

Comisia Siguranței pe net din Școala Gimnazială nr. 29, Galați este alcătuită din director prof. Dediu Cristina, director adjunct prof. Țurcanu Geanina, coordonator Comisie Esafety/Antibullying prof Caramalău Cecilia, responsabil de programe și proiecte europene (Erasmus+/Etwinning) prof. Chiroșcă Angela, consilier școlar, prof. Georgescu Victoria, profesor TIC Stanciu Adriana, Responsabil de prelucrarea datelor prof Necula Monica.

Obiectivele comisiei:

- asigurarea relațiilor pașnice, corecte, responsabile în utilizarea noilor tehnologii în școală și nu numai;
- asigurarea siguranței și securității personalului, elevilor și a părinților;
- protejarea reputației școlii;





- încurajarea elevilor de a utiliza tehnologia online într-un mod responsabil.

Politica Siguranței Online are în vedere respectarea drepturilor copilului, precum și combaterea comportamentelor antisociale și (cyber)bullying-ul. Ea a fost realizată prin implicarea și consultarea tuturor membrilor din unitatea noastră școlară: elevi, părinți, personalul școlii, reprezentanți ai comunității locale.

UTILIZAREA TELEFOANELOR MOBILE ÎN ȘCOLI

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 și 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 și bullying-ul, ele pot, de asemenea, să ofere oportunități fără precedent atunci când sunt utilizate în mod proactiv și creativ în sala de clasă, atâta timp cât există o politică strictă privind deținerea și utilizarea acestora.

În cadrul **Școlii Gimnaziale nr. 29, Galați** există o serie de reguli pentru utilizarea telefoanelor de către elevi în cadrul școlii precum:

- Elevii pot utiliza telefonul în timpul programului școlar doar cu acordul și la solicitarea profesorului pentru îndeplinirea unor sarcini, activități educaționale;
- Elevii nu au voie să utilizeze telefonul pentru a fotografia spațiul școlar, sala de clasă sau incinta școlii, fără acordul unui cadru didactic;
- În timpul programului școlar, elevii își păstrează telefonul închis, depus într-o cutie cu sertare special construită pentru acest scop;
- Elevii nu au voie să acceseze rețeaua wi-fi a școlii cu telefonul mobil; acest lucru se poate realiza doar cu ajutorul computerelor din școală atunci când este cazul.
- Se interzice categoric elevilor să acceseze conținuturi ilegale, materiale pornografice.





- Periodic, elevii vor fi informați de către cadrele didactice și profesorii diriginți cu privire la regulile de utilizare a telefoanelor mobile.
- În cadrul ședințelor cu părinții, la începutul sau pe parcursul anului școlar, aceștia vor fi informați cu privire la regulile de utilizare a telefonului mobil.
- În cazul utilizării inadecvate a telefonului, telefonul poate fi oprit de cadrul didactic care a constatat neregulile în utilizarea acestuia.
- Înainte de a fi predat profesorului, telefonul se va închide pentru protejarea datelor; dacă telefonul nu este returnat la sfârșitul zilei, părinții vor fi informați, iar telefonul se va păstra într-un loc sigur.
- În cazul nerespectării regulilor de utilizare a telefoanelor mobile, elevii vor fi sancționați în conformitate cu Regulamentul de ordine interioară al școlii, Statutul elevului, Regulamentul cadru de organizare și funcționare a unităților din învățământul preuniversitar, după cum urmează: observație individuală, muștrare scrisă, scăderea notei la purtare.

UTILIZAREA 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 conțin 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 detașabile este o sursă bine-cunoscută de infecții malware și 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 infecțiilor malware pe computerele școlii.

În cadrul Școlii Gimnaziale Nr. 29, Galați sunt dezvoltate reguli de bază privind folosirea dispozitivelor detașabile de stocare pe computerele școlii.





- Este instalat un sistem de protecție antivirus pe toate computerele din rețeaua școlară și se adoptă o practică constantă la nivel de școală în ceea ce privește protecția împotriva virusilor. Un fișier infectat de pe un dispozitiv de stocare amovibil ar putea infecta întreaga rețea școlară.

- Se solicită membrilor personalului și elevilor să scaneze toate dispozitivele detașabile împotriva programelor malware înainte de a le utiliza.

- Se permite 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-și conecteze aparatul foto sau un MP3 player-ul la un computer din rețeaua școlii, cu excepția cazului în care trebuie să facă acest lucru în cadrul unei sarcini specifice pe care au primit-o.

- Se încurajează personalul și elevii să salveze fișiere pe dispozitivele mobile pe care le folosesc pe computerele școlii doar în scopuri educaționale.

- Personalul trebuie să evite stocarea datelor sensibile ale elevilor și ale altor membri ai personalului pe dispozitive detașabile 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.

- Este instituită o procedură oficială de gestionare a incidentelor în cazul unor infecții 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.

FORMAREA – INFORMAREA PROFESORILOR PRIVIND POLITICA SIGURANȚEI ONLINE

Cercetările au demonstrat că unul dintre domeniile cheie care lipsește în școli este formarea și conștientizarea personalului din unitate.

Conducerea școlii se asigură că membrii personalului sunt informați periodic pentru a fi conștienți în legătură cu problemele Siguranței Online care-i pot afecta pe ei și pe elevii lor.





Principiile generale de formare a Siguranței Online acoperă o gamă largă de probleme și nu este abordată izolat. Personalul școlii este informat de două ori pe an sau mai des în mod excepțional, pentru a putea ține cont de schimbările suferite în obiceiurile tinerilor și în tehnologiile și aplicațiile pe care aceștia le folosesc. Deși profesorii sunt conștienți de problemele de siguranță de pe internet, unii dintre ei nu se simt pregătiți să le abordeze, având nevoie de o pregătire specială pentru a-și îmbunătăți propriile competențe digitale, precum și competențele de mediere a folosirii internetului și, implicit, pentru a-și mări încrederea în sine în ceea ce privește capacitatea lor de a ajuta copiii în acest domeniu. Acestea ar putea contribui la rândul lor la o creștere a încrederii în relația copil – profesor. Nu în ultimul rând, evoluția și dezvoltarea profesorului îl pot ajuta pe acesta să se manifeste ca un actor care folosește internetul într-un mod pozitiv și etic, devenind astfel un model real pentru copii.

Pentru a fi în concordanță cu politica de Siguranță Online a școlii, elevii trebuie permanent informați privind noile schimbări, informațiile noi privind siguranța pe internet. Pentru a fi permanent conectați profesorii din **Școala Gimnazială nr. 29, Galați** sunt informați de către coordonatorii comisiei Siguranței Online cu privire la noile reglementări care apar în fiecare an, această informare fiind punct obligatoriu în prima ședință de Consiliu Profesoral și la nevoie se fac informări și completări dacă este cazul. Informarea cadrelor didactice cuprinde:

- Informarea privind utilizarea imaginii copilului, a postării imaginii copiilor pe site-urile de socializare (cadru legal) și reamintirea semnării declarației de către orice părinte.
- Informare privind protecția datelor sensibile ale școlii și a celor personale prin crearea/reînnoirea parolelor.
- Informare privind utilizarea dispozitivelor detașabile și obligativitatea scanării fiecărui dispozitiv înaintea folosirii lui.
- Informare privind utilizarea telefoanelor ținând cont de reglementările în vigoare din ROFUIP și ROI din anul în curs.
- Informare privind procedurile de gestionare a incidentelor în cazul infectării malware dacă este cazul pentru calculatoarele școlii.





- Utilizarea calculatoarelor din clase și laboratorul doar în scopuri educative.

Recomandări privind găsirea de resurse pe site-urile oficiale **www.sigur.info**, **www.oradenet.ro**, și desfășurarea de activități anuale cu elevii.

PROTEJAREA DATELOR SENSIBILE ÎN ȘCOLI

Datele sensibile din cadrul **Școlii Gimnaziale nr. 29, Galați** includ detaliile confidențiale ale elevilor, părinților și membrilor personalului, informațiile școlare, de sănătate și psihologice ale elevilor, salariile profesorilor și CV-urile acestora, precum și date privind administrarea școlii. Aceste informații pot fi stocate pe computerele locale, pe dispozitive mobile, pe servere localizate pe teritoriul școlii sau în alte locații sau pe documente printate pe o imprimantă confidențială sau comună. Protecția insuficientă sau dezvăluirea improprie a acestor date poate rezulta într-o încălcare a confidențialității sau a legilor de protecție a datelor.

Protecția vieții private și a datelor cu caracter personal ale tuturor elevilor și personalului din școală este reglementată de legislația națională din țara noastră privind protecția datelor. Deși aceste reguli se bazează **pe o directivă europeană (95/46/EC)** există diferențe în modul în care țările au transpus acest document în legislația națională (a se consulta site-ul <https://www.dataprotection.ro/>).

În 2012, Comisia Europeană a propus o reformă majoră a Directivei Europene pentru Protecția Datelor. Noile propuneri vor consolida drepturile individule și vor aborda provocările globalizării și noilor tehnologii.

În Școala Gimnazială Nr. 29, Galați:

- Menținem două rețele separate de computere, unul destinat elevilor și profesorilor, bibliotecii, iar celălalt, pe un server de securitate, destinat treburilor administrative.





- Se actualizează sistemele de protecție antivirus pentru a evita să devenim o țintă a hackerilor.
- Criptăm și parolăm-protejăm datele sensibile și nu stocăm datele.
- Furnizăm personalului o formare de bază privind protejarea datelor sensibile;
- Creem 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.
- Nu lăsăm documente ce conțin date sensibile pe imprimanta publică sau salvate pe calculator! Distrugem/ștergem astfel de documente înainte să le punem în coșul de gunoi (Recycle Bin).
- Colectăm date sensibile doar dacă este necesar. Ceea ce nu deții, nu poate fi compromis!
- 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 atașament care oferă acces la informații confidențiale.

PROTECȚIA DISPOZITIVELOR ÎMPOTRIVA PROGRAMELOR MALWARE

Malware înseamnă software dăunător care a fost proiectat cu scopul accesării unei rețele sau unui sistem de computere fără consimțământul proprietarului și 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.).

În **Școala Gimnazială nr. 29, Galați** pe fiecare calculator este instalat firewall-ul și sisteme de protecție anti-virus și se actualizează pentru a evita breșele de securitate.





- Se blochează site-urile nedorite și ferestrele de tip pop-up prin personalizarea setărilor de securitate ale browser-ului web utilizat pe computerele școlii. Se explică elevilor de ce anume se face acest lucru și se precizează că prin aceasta se urmărește protecția lor.
- Se creează un protocol care să fie aplicat cu rigurozitate cu privire la utilizarea Internetului și verificarea mail-urilor personale pe computerele școlii.
- Nu se accesează din mail-uri adrese dubioase/reclame/pop-up oricare ce nu au legătură cu activitatea școlară.
- Nu se permite elevilor să folosească dispozitive portabile pentru a descărca fișiere de pe computerele școlii; în cazul în care acest lucru este permis trebuie să fie instruiți să scaneze mai întâi toate fișierele împotriva malware.
- Se desemnează o persoană de contact instruită să se ocupe de toate problemele legate de malware și se instituie o procedură oficială de gestionare a incidentelor informatice.

POLITICA DE UTILIZARE ACCEPTABILĂ

Reprezintă o bună practică ca toate școlile să aibă o **Politică de Utilizare Acceptabilă (PUA)**, adică un document clar și concis care să ofere îndrumare unor categorii de utilizatori cu privire la felul în care ar trebui utilizate Internetul și tehnologiile mobile. Politicile de Utilizare Acceptabilă s-au dezvoltat în timp și este evident că tinerii și personalul din școli au posibilitatea să acceseze Internetul în multe moduri, nu numai prin intermediul rețelei școlii. Având în vedere acest fapt, este important ca o Politică de Utilizare Acceptabilă **să fie centrată mai mult pe comportament decât pe tehnologie**. Acest lucru înseamnă că politica va avea o viață mai lungă și va fi mai ușor de înțeles de către toți cei interesați.





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.

- Se amintește personalului și elevilor cele 4 reguli de aur ale unui parole sigure:

1. Trebuie să fie lungă și complexă. Ideal trebuie să conțină între 10 și 14 caractere ;
2. Se folosește un amestec de numere, simboluri, litere mari și litere mici și semne de punctuație;
3. Se folosește exemplu un acronim pentru o frază, cum ar fi "Fiica mea, Harriet, este o bună metode mnemonice care să vă ajute să vă amintiți parola, de 5 jucătoare de tenis" devine FMhEObjDt sau Imi place să cânt în ploaie în fiecare zi! devine iPScipIFZ !;
4. Nu folosiți niciodată informații personale de identificare în parolă. Acestea includ nume, zile de naștere, animale de companie, adrese de străzi, școli, numere de telefon, numerele de înmatriculare etc. Acestea vor fi primele presupuneri pentru oricine încearcă să obțină acces la contul dvs.

- O parolă este ca o periută de dinți, nu trebui folosită în comun și trebuie să fie schimbată frecvent!

- Dacă utilizatorii simt totuși nevoie să scrie parola, aceasta nu trebuie să fie ținută în apropierea dispozitivului la care oferă acces.

POLITICA ȘCOLII

Politicile de Siguranței Online ale școlii 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, aceștia 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 oraș singuri sau cu prietenii lor, toate școlile trebuie să aibă o politică clară și concisă în care să se acorde atenție tuturor aspectelor Siguranței Online.





REALIZAREA ȘI PUBLICAREA DE FOTOGRAFII ȘI CLIPURI VIDEO ÎN CADRUL ȘCOLII

Participarea copiilor într-un spectacol, serbare sau într-o activitate 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 și personalul școlii ar trebui să le ia în considerare și să le comunice părinților.

Școala Gimnazială nr. 29, Galați aplică practicile:

- Școala are o politică clară referitoare la imagine.
- Comunicăm comunității școlare această politică alături de îndrumări practice clare și exemple ușor de înțeles.
- Ne asigurăm că toți părinții/tutorii legali și/sau tinerii (în funcție de vârstă și cerințe naționale) au semnat un formular de permisiune pentru foto/video ÎNAINTE de orice filmare sau fotografiere a elevilor.
- Dacă părintele nu-și dă acordul, înțelegem posibilul disconfort al elevului respectiv și ne asigurăm discret că acesta să aibă altă ocupație în timpul de filmare sau fotografiere.
- Ne asigurăm că toți membri comunității școlare înțeleg implicațiile partajării fotografiilor și conținutului video pe site-urile de socializare – nu postați NICIODATĂ numele complet, vârsta sau orice alte detalii personale alături de fotografia unui copil pe site-ul dvs.!
- Ținem minte că evenimentele școlare sunt ocazii de bucurie care nu ar trebui să fie restricționate de prea multe reglementări.





MINISTERUL EDUCAȚIEI
INSPECTORATUL ȘCOLAR JUDEȚEAN GALAȚI
ȘCOALA GIMNAZIALĂ NR. 29 GALAȚI
STR. STRUNGARIILOR, NR. 7A, COD 800 580
Telefon/Fax 0236 488560
E-mail: scoala29@yahoo.com
Site: www.scoala29gl.ro



MINISTERUL EDUCAȚIEI

DECLARAȚIE

Subsemnatul/subsemnata _____,
în calitate de părinte/tutore/reprezentant legal al minorului _____,
în vârstă de _____, declar că sunt de acord cu fotografierea și realizarea de video în
cadrul activităților desfășurate în instituția de învățământ **Școala Gimnazială nr. 29, Galați.**

Declar că nu voi avea nicio pretenție față de difuzarea fotografiilor cu minorul
reprezentat, așa cum vor fi ele difuzate conform prezentului document.

În calitate de reprezentant legal, înțeleg că pot trimite oricând organizatorului un email la
adresa scoala29@yahoo.com, prin care să solicit oprirea difuzării imaginilor cu copilul/copiii
meu/mei în viitoarele materiale promoționale sau pe internet.

Data:

Semnătura părinte.....

Director:.....





PREZENȚA ȘCOLII PE REȚELELE DE SOCIALIZARE

Folosirea rețelelor de socializare de către școli este un subiect controversat, putând fi aduce argumente pentru și împotriva, de la riscul cyberbullying-ului și prietenii online dintre elevi și profesori până la promovarea activă pe care o poate aduce Facebook sau Twitter. De dezvoltarea profesională până la descoperirea de exemple din viața reală la orele de limbi străine, socializarea media în școli poate reprezenta o resursă valoroasă. Cel mai important lucru care trebuie avut în vedere în legătură cu utilizarea rețelelor de socializare în școli este chestiunea drepturilor și responsabilităților online. Pe lângă rolul de instrument promoțional pentru școli, profesorii din toată lumea au enumerat mai jos beneficiile utilizării rețelelor sociale în școli.

Școala Gimnazială nr. 29, Galați are în vedere în acest sens:

- 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 comunității și a părinților prin intermediul grupurilor de Facebook, Pinterest, 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 împărtășirea de informații cu colegi și grupuri educaționale cu aceleași interese.
- Stabilirea de legături cu colegi din întreaga țară și chiar din lume.
- Integrarea unor exemple din lumea reală în procesul de predare.
- Rețeaua de socializare Facebook este restricționată în sălile de clasă unde se desfășoară orele de curs.





INTEGRAREA SIGURANȚEI ONLINE ÎN CURRICULUM

În ultimii ani TIC și mediul digital oferă copiilor 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 intimității lor și respectare a celui alt, de gestionare a cazurilor de cyberbullying, de a distinge între contacte și conținut nepotrivit și pozitiv, ș.a.m.d.

Școala Gimnazială nr. 29, Galați are în derulare proiect Erasmus+/concursuri naționale, proiecte eTwinning, care au la bază noile metodologii AEL, PBL, STEM, G-SUITE 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.

- Școala se asigură că Siguranța Online se predă ca parte a programei, indiferent dacă aceasta este sau nu o obligație legală în România .

- Deși predarea eSafety în cadrul cursurilor de TIC sau media pare cea mai potrivită abordare, în **Școala Gimnazială nr. 29, Galați** se urmărește o abordare trans-curriculară mai cuprinzătoare, care explorează numeroasele legături dintre eSafety și toate tipurile de conținut educațional.

- Deoarece Siguranța Online reprezintă o responsabilitate trans-curriculară, toate cadrele didactice din școală beneficiază de formare periodică pe teme cum ar fi: confidențialitatea și securitatea, amprenta digitală și reputația, cyberbullying-ul, alfabetizarea informațională etc.

- În predarea acestora și altor probleme Siguranței Online se sugerează pornind de la ceea ce elevii știu deja și de la felul în care experimentează ei mediul online.

- Încurajăm elevii să se implice în mentorat la egal la egal și facilitați discuții interactive de jos în sus.

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. Mulți părinți sunt destul de eficienți în îngrijirea și îndrumarea copiilor cu privire la problemele offline, dar sunt reticenți în încercarea de a le oferi sprijin similar în ceea ce privește aspectele digitale ale vieții lor. Parțial acest lucru poate fi un rezultat al faptului că mulți părinți spun despre copiii lor că "se pricepe mai bine la tehnologie" decât ei.

Școala Gimnazială nr. 29, Galați oferă sprijin, îndrumare și consiliere pentru părinți. Acest lucru poate lua diverse forme, o discuție specifică pe această temă, pliante despre diferite probleme, legături (link-uri) pe site-ul școlii sau un articol în buletinul online al școlii, informări în ședințe cu părinții.

- Părinții interesați de ceea ce fac copiii lor aceștia se confruntă online și vor fi dornici să comunice pe aceste teme, vor fi, de asemenea, mult mai conștienți cu privire la problemele actuale ale siguranței pe internet.

- **Școala Gimnazială nr. 29, Galați** raportează că implicarea părinților în problemele eSafety poate fi o provocare și că aceștia sunt de multe ori reticenți 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 înclinați să vină la un eveniment în care copilul lor participă direct, de exemplu, prin susținerea unei prezentări.

- O altă strategie este livrarea mesajelor eSafety în timp ce părinții sunt deja în școală cu alte scopuri, ședințe cu părinții, lectorate pe școală, întruniri ale părinților din **Asociația părinților a Școlii Gimnazială nr. 29, Galați** distribuie de fluturași, flyere despre diferite aspecte ale siguranței în mediul on-line, promovarea de link-uri pe pagina de facebook a școlii, pe site-ul școlii, articole în revista școlii.





UTILIZAREA TEHNOLOGIEI ONLINE DE CĂTRE ELEVI ÎN AFARA ȘCOLII

Incidentele online care au loc în afara școlii vor avea în mod inevitabil un impact în interiorul școlii. Cele mai frecvente probleme cu care s-ar putea confrunta **Școala Gimnazială Nr. 29, Galați** sunt spargerea conturilor, încălcarea confidențialității, sexting, utilizarea excesivă și cyberbullying-ul. Este important pentru o școală să stabilească dacă și cum dorește să răspundă la astfel de evenimente.

Practicile pe care **Școala Gimnazială Nr. 29, Galați** le abordează în acest caz:

- Includem o declarație în Politica școlii și în Politica de Utilizare Acceptabilă cu privire la modul în care vor fi gestionate problemele online care au loc în afara școlii.
- Informăm foarte bine părinții și elevii cu privire la angajamentul școlii de a se ocupa de aceste tipuri de probleme.
- Organizăm în cadrul școlii, activități de creștere a gradului de conștientizare pentru a informa elevii de posibilele consecințe ale problemelor online, cum ar fi bullying-ul și încălcarea confidențialității. Solicităm feedback de la elevi pentru a vedea ce tip de sprijin suplimentar eSafety ar trebui să li se ofere în afara programei.
- Desemnăm un profesor sau consilier pe care elevii îl pot consulta atunci când se confruntă cu probleme online, indiferent dacă acestea au loc la școală sau în afara școlii. Această persoană ar trebui să fie în măsură să ofere sfaturi tehnice de bază (de exemplu, cum pot să-mi protejeze contul de Facebook), precum și consiliere psihologică (de exemplu, în cazul unui incident de cyberbullying).
- Atunci când este necesar, **Școala Gimnazială Nr. 29, Galați** trebuie să contacteze părinții tuturor elevilor implicați într-o problemă și dacă este cazul să apeleze la ajutor profesionist extern.
- Urmărim numărul și natura rapoartelor și identificăm eventualele nevoi specifice din școală.





GESTIONAREA INCIDENTELOR

În toate școlile au loc incidente și acestea pot apărea în multe domenii diferite - de la un virus sau atac împotriva serverelor școlii până la incidente de cyberbullying. Din păcate, incidentele nu sunt privite întotdeauna ca o oportunitate de a învăța.

Școala Gimnazială nr. 29, Galați are în vedere următoarele practici :

- Se aplică procedura de gestionare a incidentelor care face parte din Politica școlii , astfel că fiecare membru al personalului să știe ce este de făcut în cazul unui incident.
- Revizuim incidentele la ședințele periodice cu personalul. Imediat după incident ar putea exista o rezistență firească la revizuirea incidentului din partea membrilor personalului implicat. Lăsăm să treacă un timp, astfel încât toată lumea să privească incidentele cu detașare.
- Discutați întrebările din lista de control eSafety atunci când revizuim un incident.
- Raportăm incidentul prin intermediul incident handling report. (*Raportarea incidentelor prin intermediul unui șablon furnizat pe site va conta în acordarea punctelor de acreditare, va rămâne anonimă și ne va ajuta pe toți să învățăm unii de la alții.*)

CYBERBULLYING

Cyberbullying – denumit uneori și bullying online; este o problemă foarte complexă. Poate fi definit ca utilizarea tehnologiei și în special a telefoanelor mobile și Internetului, pentru a răni în mod deliberat, supăra, hărțui sau a jena o persoană. Acesta poate fi prelungire a intimidării față-în-față, tehnologia oferind agresorului o altă metodă de hărțuire a victimei, sau fără niciun motiv. Poate avea loc prin intermediul oricărei forme de media, de la mesaje și imagini ofensatoare trimise de pe telefoane mobile, la postări neplăcute pe bloguri și pe rețelele de socializare sau e-mailuri și mesagerie instantanee, până la site-uri dăunătoare create numai cu scopul de a intimida o persoană sau abuz virtual în timpul unui joc multiplayer online.

Cyberbullying-ul diferă de alte forme de bullying: poate invadea casa și spațiul personal al victimei, publicul este potențial mai numeros, mesajele sau imaginile supărătoare pot fi





propagate rapid și există dificultăți în controlarea și/sau eliminarea mesajelor transmise electronic.

De asemenea, deoarece nu presupune interacțiune față-în-față, cyberbullyingului i se atribuie de obicei un caracter anonim. Acest lucru îi poate determina pe oameni să se implice în activități în care nici n-ar visa să se implice în lumea reală, fie ca autor sau ca un spectator.

Se adoptă o abordare anti-bullying la nivelul **Școlii Gimnaziale Nr. 29, Galați**, astfel:

- Comunicăm în mod clar strategia pentru toți membrii comunității școlare - elevi, cadre didactice, personal adițional și părinți. Toată lumea este conștientă de traseele de raportare și de consecințele pentru cei implicați în astfel de comportamente.

- Se revizuieste periodic strategia adoptată, se evaluează succesul acesteia și o adaptăm dacă este necesar.

- Organizăm și încurajăm formări pentru profesori.

- Integrăm în programă conștientizarea cu privire la (cyber)bullying pentru toate categoriile de vârstă.

- Organizăm sesiuni de informare pentru părinți. Aceștia ar putea să nu fie conștienți de noile instrumente tehnologice și de modul în care copiii lor le folosesc.

ANTI-SEXTING

Sextingul pare a fi o problemă care apare constant la știri. Este definit ca schimbul de mesaje sau imagini cu caracter sexual și crearea, partajarea și transmiterea de imagini nud cu conotație sexuală sau imagini semi-nud prin intermediul telefoanelor mobile sau internet.

Cercetările sugerează că sextingul a devenit o practică obișnuită în rândul tinerilor de azi. Caracterul omniprezent al tehnologiei de astăzi și în special al telefoanelor mobile face ca tinerii să aibă acces la camere foto și să poată face poze oricând doresc și, uneri, ei pot lua decizii greșite. Este important de reținut că nu doar tinerii cad victime sextingului, ci chiar cântăreța Tulisa de la N-Dubz a spus că a fost „trădată, devastată și cu inima zdrobită” atunci când fostul ei prieten a postat videoclipuri intime online.





În unele țări există consecințe legale pentru sexting și, în multe cazuri, fotografia nud a unei persoane sub 18 ani este clasată ca fiind o imagine ilegală sau o imagine care înfățișează abuz sexual asupra copilului. Acest lucru înseamnă că potențialele consecințe pot fi severe și, unii ar spune, disproporționate.

Așadar, **Școala Gimnazială Nr. 29, Galați** are în vedere protejarea în acest sens a copiilor:

- Ne asigurăm că sextingul și abordarea în privința lui este înțeleasă de toată lumea și acest lucru se reflectă în politica de protecție a copilului.
- Oferim copiilor oportunități de a discuta despre subiecte precum sextingul.
- Furnizăm training și informări personalului pentru ca aceștia să fie conștienți de ricurile și provocările legate de sexting.
- Furnizăm informații pentru părinți și acceptăm faptul că aceștia ar putea fi șocați dacă vor afla că și copii lor sunt implicați în sexting.

Director:

Prof. Dediu Cristina

Întocmit:

Comisia Antibullying Siguranța Online
Coordonator Prof. Țurcanu Geanina





II. POLITICA DE UTILIZARE ACCEPTABILĂ DE TIC DE CĂTRE PERSONAL ȘCOLII GIMNAZIALE NR. 29, GALAȚI

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 școlii 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 Informaționale și de Comunicare, membrii personalului sunt rugați să citească și să semneze *Politica de Utilizare Acceptabilă (PUA)*.

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

- 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 și site-uri de socializare.
- Sistemele de informare deținute de școli trebuie să fie utilizate în mod corespunzător. Înțeleg că următoarele infracțiuni pot să contravină legislației în vigoare: obținerea accesului neautorizat la date informatice; obținerea accesului neautorizat la date informatice cu intenția de a comite sau facilita comiterea altor infracțiuni sau de a modifica datele informatice fără autorizare.
- 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 informațional nesupravegheat fără să mă deconectez în prealabil sau fără să blochez accesul în mod corespunzător.

- Voi respecta securitatea sistemului și nu voi dezvălui nicio parolă sau informații de securitate. Voi folosi o parola "puternică" (o parolă puternică conține 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).
- Nu voi încerca să instalez niciun program software achiziționat sau descărcat, inclusiv toolbar-uri sau hardware fără permisiunea managerului de sistem.
- Mă voi asigura că toate datele cu caracter personal ale elevilor, personalului sau părinților/tutorilor sunt păstrate în conformitate cu **Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date**.
- Aceasta înseamnă că toate datele cu caracter personal vor fi obținute și prelucrate în mod corect și legal și vor fi păstrate în confidențialitate și 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 școlii (cum ar fi prin e-mail sau pe memory stick-uri sau CD-uri) vor fi criptate printr-o metodă aprobată de către școală (vezi *Politica de securitate a datelor*). Orice imagini sau clipuri video ale elevilor vor fi folosite numai în concordanță cu politica școlii de utilizarea a imaginii (vezi *Politica de utilizare a imaginilor*) și se va lua întotdeauna în considerare consimțământul părinților.
- Nu voi păstra documente profesionale ce conțin informații sensibile sau cu caracter personal legate de școală (inclusiv imagini, fișiere video etc.) pe orice dispozitiv personal (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 Școlii 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.
- Nu voi utiliza sistemul informatic al școlii pentru a stoca informații personale fără legătură cu activitățile școlare, cum ar fi fotografiile personale, fișiere și informații financiare.
 - Voi respecta drepturile de proprietate intelectuală și drepturile de autor.
 - Am citit și am înțeles politica de Siguranței Online a școlii 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 elevilor în clasă și în alte spații de lucru.
 - Voi raporta coordonatorului Comisiei Antibullying - Siguranței Online dir. adj. prof. Țurcanu Geanina, toate incidentele îngrijorătoare cu privire la siguranța online a copiilor, cât mai curând posibil. Voi raporta orice acces accidental, primirea de materiale nepotrivite, breșe de securitate sau site-uri nepotrivite către coordonatorul eSafety, cât mai curând posibil.
 - Nu voi încerca să ocolesc filtrele și/sau sistemele de securitate implementate de către școală. 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 sau doamnei director cât mai curând posibil.
 - Comunicarea electronică cu elevii, părinții/tutorii și alți se va desfășura numai prin intermediul canalelor de comunicare aprobate de școală (de ex. prin intermediul adresei personale de email sau prin secretariat care va folosi adresa de email a școlii (scoala29@yahoo.com). Orice relații pre-existente ce ar putea compromite acest lucru vor fi discutate cu echipa de conducere.
 - Utilizarea TIC și a sistemelor informatice va fi întotdeauna compatibilă cu rolul meu profesional, fie că utilizez sisteme personale sau sistemele școlii. 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 școlii și cu legea. Nu mă voi împrieteni cu elevii pe site-uri de socializare de tip Facebook.

- Nu voi crea, transmite, afișa, publica sau trimite mai departe orice material ce poate harțui, ofensa, deranja sau cauza anxietăți inutile oricărei alte persoane, sau orice material care ar putea compromite rolul meu profesional, școala sau Consiliul Județean.
- Voi promova eSafety în rândul elevilor aflați sub supravegherea mea și îi voi ajuta să dezvolte o atitudine responsabilă referitoare la siguranța online, utilizarea sistemului și conținutul pe care îl accesează sau îl creează.
- Dacă am nelămuriri sau întrebări cu privire la siguranță și practica profesională online, fie în școală, fie în afara școlii, le voi aduce la cunoștința coordonatorului Siguranței Online prof. Țurcanu Geanina sau a directorului școlii.
- Înțeleg că utilizarea a sistemelor informatice, a Internetului și e-mailului poate fi monitorizată și înregistrată în vederea asigurării respectării politicii.

Școala își poate exercita dreptul de a monitoriza utilizarea sistemelor informatice, inclusive accesul la Internet, în scopul monitorizării respectării Politicii de Utilizare Acceptabilă și Politicii de Securitate a Datelor. În cazul în care se consideră că are loc folosirea neautorizată și/sau necorespunzătoare a sistemului informatic al serviciului sau un comportament inacceptabil sau necorespunzător, școala va invoca procedura sa disciplinară. Dacă școala 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.





III. PLANUL DE ACȚIUNE SIGURANȚEI ONLINE A ȘCOALA GIMNAZIALĂ NR. 29, GALAȚI

INFRASTRUCTURĂ

Securitate tehnică

Toate computerele importante ale școlii sunt protejate împotriva virușilor. Ne-am asigurat să includem un paragraf privind protecția antivirus în Politica Școlii și în Politica de Utilizare Acceptabilă, și ne-am asigurat că personalul și elevii aplică în mod riguros îndrumările școlii.

Avem un bun grad de filtrare în școala noastră. Luăm în considerare, unde este necesar, o filtrare diferențiată în funcție de nevoile diferiților elevi. În cazul de utilizatori care accesează conținut inadecvat, atunci se ia în considerare o filtrare adițională sau educație suplimentară (sau ambele). O abordare educațională eficientă și creșterea încrederii elevilor de toate vârstele sunt esențiale pentru utilizarea mediului online în condiții de siguranță și responsabilitate, astfel este recomandat să reuniți toate cadrele didactice pentru o discuție privind modul în care să se discute cu elevii despre cum să fii un bun cetățean digital, (<https://www.betterinternetforkids.eu/web/portal/resources/gallery>), pentru exemple discuții care pot avea loc în sala de clasă pe acest subiect, prin exemple de lecții, jocuri de rol și de grup.

Accesul elevilor și profesorilor la tehnologie

Tuturor membrilor personalului și elevilor li se permite să folosească stick-uri USB de memorie în școală. Aceasta este o practică bună și Politica de Utilizare Acceptabilă stipulează că toate mediile amovibile trebuie verificate înainte de utilizare în sistemele școlii. Se consultă fișa informativă pentru Utilizarea dispozitivelor mobile la





<https://www.esafetylabel.eu/group/community/use-of-removable-devices> pentru a se asigura că acoperim toate aspectele legate de securitate.

Deoarece personalul și elevii pot folosi propriul echipament în rețeaua școlară, este important să ne asigurăm că Politica de Utilizare Acceptabilă este revizuită în mod regulat de către toți membrii școlii și adaptată, dacă este necesar. Se discută cu elevii la începutul anului școlar, astfel încât aceștia să înțeleagă regulile care le protejează confidențialitatea și motivele pentru care acestea sunt instituite. Ne bazăm pe Politica în jurul comportamentului, mai degrabă decât pe tehnologie. Vizitatorii trebuie să citească și să semneze Politica de Utilizare Acceptabilă înainte de a folosi rețeaua școlii.

Protecția datelor

Avem o politică de protecție a datelor utilizatorilor în mediul școlar, protecția datelor elevilor și personalului. Pentru aceasta ne asigurăm că toți utilizatorii respectă și au înțeles regulile în cazul accesării conținuturilor nepotrivite sau ilegale de pe sistemul informatic al școlii. De asemenea avem o politică bună de gestionare separată a mediilor de învățare și de administrare. Instruirea personalului este actualizată în vederea gestionării acestor medii, pe măsură ce ne revizuim politicile. Împărtășim politica cu alți utilizatori eSafety prin încărcarea ei pe profilul școlii.

Noii utilizatori primesc o parolă standard și li se cere să-și genereze propria parolă la primul acces. Parolele oferă puncte unice în acces în sistemul informatic al școlii și de aceea trebuie respectate riguros câteva reguli privind securitatea parolei.

Licențe software

Școala noastră a stabilit un buget realist pentru programele de software. Ne asigurăm că va rămâne așa. Putem, de asemenea, să căutăm alternative, spre exemplu servicii Cloud sau software gratuite (open-source).





Ne asigurăm că toți noii angajați sunt informați în legătură cu procedurile necesare instalării de software nou. Acest lucru va însemna că securitatea sistemului poate fi menținută și că personalul poate încerca noi aplicații software, lucru care va ajuta la procesul de predare și învățare. Desemnăm o persoană specializată în domeniul IT, care se ocupă de acest lucru astfel încât să nu fie compromis sistemul de securitate al școlii.

Management IT

Este o bună practică să ne asigurăm că persoana responsabilă cu IT este pe deplin informată cu privire la programele instalate pe calculatoarele școlii. Acest lucru este indicat în mod clar în Politica școlii și în Politica de Utilizare Acceptabilă. Persoana responsabilă cu rețeaua IT este în măsură să garanteze conformitatea cu cerințele de licențiere și, de asemenea, că noul software nu va interfera cu funcționalitatea rețelei.

Deși doar directorul împreună cu responsabilul IT pot instala hardware/software în școală, se are în vedere și oportunitatea altor membri de a instala software dar numai cu acordul și suportul acestora, fără a afecta rețeaua de informatică de securitate. Ne asigurăm că toți noii angajați sunt informați în legătură cu procedurile necesare instalării de software nou. O dată pe an se iau decizii privind achiziționarea de hardware/software nou. Găsim metode de a permite cererilor de achiziționare hardware/software să fie făcute și pe tot parcursul anului. Acest lucru va permite profesorilor să creeze lecții interactive fără tentația de a folosi materiale aflate sub incidența drepturilor de autor.

POLITICĂ

Politica de Utilizare Acceptabilă (PUA)





Avem o Politică de Utilizare Acceptabilă pentru toți membrii comunității școlii. Revizuim în mod regulat PUA pentru a ne asigura că aceasta este încă adaptată scopului. Ne asigurăm că Politică de Utilizare Acceptabilă este adusă spre informare profesorilor și elevilor prin luare la cunoștință și mai mult, este discutată cu aceștia înainte de a fi semnată.

Revizuim anual politica de Utilizare a telefoanelor mobile în școli. Schimbările sunt incluse imediat în politicile școlii. Luăm în considerare că și schimbările din afara școlii, precum și noile tehnologii, pot afecta politicile. Din acest motiv, ne revizuim politicile anual.

Raportarea și abordarea incidentelor

Tot personalul este familiarizat cu procedura de gestionare a materialelor potențial ilegale. Există o persoană desemnată din echipa de conducere a școlii care își asumă întreaga responsabilitate în acest caz. Procedura este comunicată în mod clar către întregul personal prin Politică școlii și către profesori și elevi prin Politică de utilizare Acceptabilă. Raportăm orice conținut ilegal pe site-ul dvs național INHOPE (www.inhope.org).

Înregistrarea centralizată a incidentelor cyberbullying care au loc în școală reprezintă o bună practică. În acest fel contribuim la construirea unei baze de date cu practice de succes în gestionarea incidentelor din întreaga Europă, pe care noi și alții o putem folosi în viitor. Ne asigurăm că elevii aderă la îndrumările anti-cyberbullying din Politică de Utilizare Acceptabilă.

Politica Personalului

Politica de Utilizare Acceptabilă conține îndrumări privind utilizarea telefoanelor mobile la clasă de către cadrele didactice.

Comportamentul și practica elevilor/Prezența online a Școlii

Am definit standardele comunicării electronice în Politică de utilizare Acceptabilă și acest lucru este un exemplu de bună practică. Am realizat o prezentare despre protecția online a





elevilor și pericolele posibile la accesarea mediului online, încărcată pe profilul școlii noastre, permițând și altor școli să beneficieze de experiența noastră. Școala abordează în totalitate consecințele pozitive și negative ale comportamentului elevilor.

În cadrul școlii este desemnată o persoană responsabilă cu monitorizarea online a reputației școlii (site-ul școlii și prezența școlii în rețeaua Facebook) și care intervine prompt în cazuri neconforme sau postări care dăunează imaginii școlii sau afectează negativ comportamentul elevilor sau personalului școlii.

Este bine că elevii pot da feedback cu privire la prezența școlii în mediul online. Luăm în considerare crearea unui spațiu gestionat integral de elevi. Este o oportunitate grozavă de învățat competențe digitale. Avem în vedere o rețea de colegi care să ofere suport elevilor.

PRACTICĂ

Management

Pe lângă o desemnare clară a responsabilităților, pentru a ne asigura că totul este în regulă cu securitatea rețelei și confidențialitatea utilizatorilor, este esențial ca în școală să aibă loc audituri și controale procedurale regulate. Fără aceasta, școala va deveni vulnerabilă. Deși în școală există o persoană responsabilă cu problemele Siguranței Online, toată lumea trebuie să împartă responsabilitatea asigurării datelor sensibile utilizate în îndatoririle profesionale de zi cu zi. Chiar și personalul neimplicat direct în manipularea datelor este constient de riscuri și amenințări, precum și de modalitățile de minimizare a problemelor.

Noile tehnologii se dezvoltă rapid și este necesar să fim la curent cu noile tendințe informatice pentru protejarea membrilor școlii și în special a elevilor, de aceea este impetuos a urmării noutățile în domeniu pe portalul specializat <https://www.betterinternetforkids.eu/>, unde întregul personal poate lua parte la diverse metode de informare, cursuri online sau seminarii legate de riscurile mediului online și prevenirea incidentelor în rândul tinerilor.

