



Liceul Teoretic "Aurel Lazăr"

Str. Avram Iancu Nr. 10, 410094 Oradea, Bihor
Tel : 00 40 259 436208; 00 40 259 434019
00 40 359 410526; 00 40 359 410527
Fax: 00 40 259 436208; 00 40 259 434019
E-mail: alazar1990@yahoo.com
www.alazar.ro

POLITICA SECURITĂȚII INFORMATICE (eSafety)

Siguranța online este parte integrantă a mai multor politici ale Liceului Teoretic "Aurel Lazăr". Aspecte privind siguranța online se regăsesc în documente cum ar fi: *Planul de dezvoltare instituțională*, *Planul managerial*, *Planurile manageriale ale comisiilor de lucru*, *procedurile interne ale școlii*, *Regulamentul de ordine interioară* și *Planul de Acțiune eSafety* al școlii.

1. ARGUMENT

Politica eSafety este necesar a fi elaborată și implementată în școală deoarece internetul, telefoanele, mijloacele digitale se utilizează permanent la fiecare nivel: elevi, profesori, personal auxiliar. Pentru a ne asigura că toți factorii implicați în educație știu să utilizeze corect și sigur oportunitățile oferite de tehnologia digitală, ei trebuie să înțeleagă și să știe să o folosească într-un mod sigur oriunde.

2. RESPONSABILITĂȚI

La nivelul liceului comisia pentru siguranța în mediul online este constituită din directorul unității, profesorii de informatică/TIC, inginerul de system și consilierul educativ. Aceștia se ocupă de implementarea și monitorizarea politicii eSafety a școlii, raportând după caz directorului, diriginților sau profesorilor orice schimbare importantă în utilizarea tehnologiei, noile reglementări eSafety sau dacă este cazul discută evenimente care se petrec în școală privind acest aspect, precum și organizarea evenimentelor cu ocazia **Zilei Europene a siguranței pe internet** (februarie), precum și din cadrul **Lunii europene a securității cibernetice** (octombrie) care este o campanie anuală a Uniunii Europene menită să sensibilizeze cetățenii și organizațiile cu privire la securitatea cibernetică prin furnizarea de informații la zi din domeniul securității prin intermediul educației și al schimbului de bune practici.

Comisia eSafety este alcătuită din:

- prof. Gheorghe Tirla – director
- prof. Viorel Muscaș – prof. informatică
- prof. Rodica Berdie – prof. informatică
- ing. Ovidiu Hanga – inginer de sistem
- prof. Elena Luca – consilier educativ

Siguranța în mediul online reprezintă o responsabilitate pentru orice profesor al școlii.

3. OBIECTIVE

Politica eSafety a școlii are următoarele obiective:

- 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 eSafety este elaborată în acord cu legislația națională și internațională, cu politicile școlii, are în vedere respectarea drepturilor copilului, precum și combaterea comportamentelor antisociale și bullying-ul. Ea a fost realizată prin implicarea și consultarea tuturor – elevi, părinți, personalul școlii, reprezentanți ai comunității locale.

4. UTILIZAREA TELEFOANELOR MOBILE ÎN ȘCOALĂ

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. (ROFUIP, art. 197, 2)

La Liceul Teoretic “Aurel Lazăr” 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 închisă în dulapul clasei;
- 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 reținut 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*.

5. 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 binecunoscută 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 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 virușilor. 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.

6. FORMAREA – INFORMAREA PROFESORILOR PRIVIND POLITICA eSAFETY

Pentru a fi în concordanță cu politica eSafety a școlii, elevii trebuie permanent informați privind noile schimbări, informațiile noi privind siguranța pe internet. Pentru a fi permanent conectați profesorii sunt informați de către coordonatorii comisiei eSafety 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 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 înainte de folosirea 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 și desfășurarea de activități anuale cu elevii.

De asemenea, profesorii sunt invitați să participe la evenimentele organizate în cadrul Lunii europene a securității cibernetice și cu ocazia Zilei Siguranței pe Internet.

7. PROTEJAREA DATELOR SENSIBILE ÎN ȘCOALĂ

Datele sensibile din cadrul unei școli 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.

DECI

- În școală se actualizează sistemele de protecție antivirus pentru a evita să deveniți o țintă a hackerilor.
- Nu se vor lăsa documente ce conțin date sensibile pe imprimanta publică sau salvate pe calculator! *Distrugeți/ștergeți astfel de documente înainte să le puneți în coșul de gunoi (Recycle Bin).*
- Colectați date sensibile doar dacă este necesar. 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.

8. 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 informatici 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.).

AȘADAR

- În școală 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 orice care 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 care să se ocupe de toate problemele legate de malware și se instituie o procedură oficială de gestionare a incidentelor informatice.

9. POLITICA DE UTILIZARE ACCEPTABILĂ

Reprezintă o bună practică ca școala 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 elevii 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.

10. 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:

- să conțină între 10 și 14 caractere;
- folosirea unuu amestec de numere, simboluri, litere mari și litere mici și semne de punctuație;
- folosirea unui acronim pentru o frază;

- să nu se utilizeze 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.); dacă utilizatorii simt totuși nevoie să scrie parola, aceasta nu trebuie să fie ținută în apropierea dispozitivului la care oferă acces.

11. POLITICA ȘCOLII

Politicile de eSafety 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 elevi, 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, școala trebuie să aibă o politică clară și concisă în care să se acorde atenție tuturor aspectelor eSafety.

12. REALIZAREA ȘI PUBLICAREA DE FOTOGRAFII ȘI CLIPURI VIDEO ÎN CADRUL ȘCOLII

Participarea elevilor la anumite activități și evenimente reprezintă momente de neuitat și motive de mândrie pentru părinți – sunt momente pe care mulți vor dori să le fotografieze sau să le 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.

DREPT URMARE, conducerea, cadrele didactice și personalul școlii trebuie:

- Să știe că școala are o politică clară referitoare la imagine și fotografie indiferent dacă aceasta este sau nu o obligație legală în țară.
- Se comunică comunității școlare această politică alături de îndrumări practice clare și exemple ușor de înțeles.
- Să se asigure că toți membri comunității școlare înțeleg implicațiile partajării fotografiilor și conținutului video pe site-urile de socializare – a nu se posta NICIODATĂ numele complet, vârsta sau orice alt detaliu personal alături de fotografia unui copil pe site.

- Să se asigure că toți părinții/tutorii legali și/sau elevii (în funcție de vârstă și cerințe naționale) au semnat un formular de permisiune (declarație) pentru foto/video ÎNAINTE de orice filmare sau fotografiere a elevilor, după modelul:

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 Liceul Teoretic “Aurel Lazăr” din orașul Oradea, județul Bihor.

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 e.mail la adresa alazar1990@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,

Prof.....

13. 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-ul sau Twitter-ul. De la 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:

- 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, 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 împărtășirea de informații cu colegi și grupuri educaționale cu aceleași interese.
- Stabilirea de legături cu colegi din țară, din Europa și 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.

14. INTEGRAREA eSAFETY ÎN CURRICULUM

În ultimii ani TIC și mediul digital oferă elevilor – copiii 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 găsim a unui echilibru între oportunități și riscuri, de gestionare a informațiilor online și a securității acestora, de protejare a intimității lor și respectare a celuiilalt, de gestionare a cazurilor de cyberbullying, de a distinge între contacte și conținut nepotrivit și pozitiv, ș.a.m.d. Liceul Teoretic “Aurel Lazăr” are în derulare multiple proiecte (locale, naționale, și internaționale) 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.

ÎN CONSECINȚĂ

- Școala se asigură că eSafety se predă ca parte a programei (indiferent dacă aceasta constituie sau nu o obligație legală în România).
- Deși predarea eSafety în cadrul cursurilor de TIC sau media pare cea mai potrivită abordare, în școală se urmărește o abordare trans-curriculară mai cuprinzătoare, menită a explora numeroasele legături dintre eSafety și toate tipurile de conținut educațional.
- Deoarece eSafety 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 aspect referitoare la eSafety trebuie pornit de la ceea ce elevii știu deja și de la felul în care experimentează ei mediul online.
- Elevii trebuie să se implice în mentorat de la egal la egal și să se faciliteze discuțiile interactive de jos în sus.

15. INFORMAȚII PENTRU PĂRINȚI

Părinții joacă un rol vital în siguranța online a copiilor și tinerilor. Desigur, școala este în măsură să adopte multe măsuri – poate filtra, monitoriza și educa, dar trebuie să recunoaștem că mulți elevi 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 pricep mai bine la tehnologie” decât ei.

- Liceul Teoretic “Aurel Lazăr” 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 articole în revista școlii “Lăzăriștii”, informări în ședințe cu părinții.
- Este important să recunoaștem că de multe ori părinții care participă la o activitate sau eveniment eSafety sunt tocmai părinții care probabil nu au nevoie să participe. Părinții interesați de ceea ce fac copiii lor online vor fi dornici să comunice pe aceste teme, vor fi, de asemenea, mult mai conștienți cu privire la problemele actuale ale siguranței pe internet.
- Școlile 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 elevilor 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, sedințe cu părinții, lectorate pe școală, întrunirile părinților din Asociația “Parentes”, distribuire 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.

16. 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 o școală sunt spargerea conturilor, încălcarea confidențialității, sexting, utilizarea excesivă și cyberbullyingul.

Este important pentru școală să stabilească dacă și cum dorește să răspundă la astfel de evenimente.

Modalități:

- Includerea unei declarații 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.
- Oferirea de Informații părinților și elevii cu privire la angajamentul școlii de a se ocupa de aceste tipuri de probleme.
- Organizarea în cadrul școlii a unor 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.
- Solicitarea unui feedback de la elevi pentru a vedea ce tip de sprijin suplimentar eSafety ar trebui să li se ofere în afara programei.
- Desemnarea unui profesor 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 trebuie 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).
- La nevoie, școală trebuie să contacteze părinții tuturor elevilor implicați într-o problemă și dacă este cazul să apeleze la ajutor profesionist extern.
- Urmărirea numărului și natura rapoartelor și identificarea eventualelor nevoi specifice din școală.

17. 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.

ÎN ACEST SENS

- Este important să se revizuiască incidentele la ședințele periodice cu personalul. (imediat după incident ar putea exista o rezistență firească la revizuirea incidentului din partea membrilor personalului implicat. Este preferabil a se lăsa un timp de reflexie, astfel încât toată lumea să privească incidentele cu detașare.)
- Este necesară discutarea întrebărilor din lista de control eSafety atunci când se revizuieste un incident. (Incidentul trebuie raportat prin intermediul handling report.)
- Raportarea incidentelor prin intermediul unui șablon furnizat pe site va conta în acordarea punctelor de acreditare, va rămâne anonimă și va constitui o sursă de învățare unii de la alții.)

18. 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, cu 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 invada 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.

PENTRU EVITAREA ACESTOR SITUAȚII

- Se adoptă o abordare anti-bullying la nivelul întregii școli.

- Se comunică în mod clar strategia pentru toți membrii comunității școlare – elevi, cadre didactice, personal adițional și părinți. Toată lumea trebuie să fie 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 se adaptează dacă este necesar.
- Se organizează sau se încurajează participarea la formări pentru profesori.
- Se integrează în programă conștientizarea cu privire la (cyber) bullying pentru toate categoriile de vârstă.
- Se organizează 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.)

DIRECTOR,
Prof. Gheoghe TIRLA

ANEXA 1

eSAFETY

RECOMANDĂRI PENTRU ELEVII DE GIMNAZIU

“Noile tehnologii devin din ce în ce mai accesibile pentru toate gospodăriile. Copiii au acum acces la internet și ‘decalajul digital’ dintre părinți și copii expune mulți tineri pericolelor din internet”, explică Luis Corrons, director tehnic al Panda Security. “Trebuie să ne asigurăm că tinerii se pot bucura de Web într-un mod sănătos și sigur. Întotdeauna am recomandat ca cea mai bună formă de a face asta este printr-o relație elev – profesor sau elev – părinte bazată pe încredere, ceea ce ar elimina necesitatea monitorizării constante a copiilor când navighează pe internet sau când intra pe rețelele sociale”.

Nu accesați niciodată linkuri suspecte.

Când folosiți programe de mesagerie instant (cum ar fi Yahoo Messenger, MSN sau orice altă aplicație de chat) sau când veți primi un e-mail, nu accesați niciodată link-ul direct din aceste programe. Dacă mesajul sau e-mailul vine direct de la cineva cunoscut, atunci tastați adresa în browser. În cazul în care nu cunoașteți persoana de la care vine mesajul atunci cel mai bine este să-l ignorați.

Este periculos să descarcați sau să rulați fișiere din surse necunoscute.

Fără îndoială ați primit de multe ori mesaje instant invitându-vă să descărcați o fotografie, o melodie sau un clip video. Uneori, acest fișier ar fi putut fi trimis nu de către acea persoană, ci de un program malițios care a infectat computerul acestuia și care încearcă să se răspândească la alți utilizatori. În această situație cel mai bun lucru pe care îl puteți face este să vă întrebați prietenii dacă au trimis într-adevăr ceva. Dacă nu, informați-i că sunt infectați astfel încât să poată șterge fișierul și să-și informeze celelalte contacte din listă.

Nu vorbiți cu străinii.

În camere chat, pe rețelele sociale sau pe messenger, nu puteți fi niciodată complet sigur cu cine stați de vorbă atâta timp cât nu va puteți vedea. În special în comunitățile online sunt oameni care nu s-au întâlnit în viața reală. Niciodată să nu vă împrieteniți cu străinii și în nici

un caz nu ar trebui să vă aranjați vreodată întâlniri în viața reală.

Nu trimiteți informații confidențiale prin internet.

Nu trimiteți niciodată informații personale (adresă, număr de telefon etc.) prin email sau instant messaging și nu publicați aceste informații pe bloguri sau forumuri. De asemenea, trebuie să fiți atenți când vă creați profile pe rețele sociale, cum ar fi Facebook sau Myspace. Nu ar trebui să divulgați informații ca vârsta sau adresă. Este recomandat să nu folosiți numele vostru adevărat, ci un pseudonim sau poreclă.

Dacă aveți cea mai mică bănuială, fiți prudenți.

Dacă un program pe care nu vă amintiți că l-ați instalat începe să afișeze avertizări de infecții sau ferestre care vă invită să cumpărați anumite produse, aveți mare grijă. Este posibil să fiți infectat cu unele programe malware.

Nu navigați singuri pe internet.

Dacă vreți să căutați ceva pe internet, este mult mai bine să cereți ajutorul sau sfatul unui adult, în ceea ce privește locurile în care să căutați. Este pe departe mult mai sigur și vizitați site-uri sigure și oficiale, în comparație cu pagini web necunoscute.

Vorbiți cu profesorii, părinții sau tutorii voștri.

Dacă aveți orice întrebare pe acest subiect, dacă observați ceva suspect sau primiți mesaje ofensatoare sau periculoase, luați imediat legătura cu un adult. Ei vor fi în măsură să vă sfătuiască.

ANEXA 2

ȘCOALA ȘI COMPETENȚELE NECESARE ÎN SECOLUL XXI

Forța motrice a secolului XXI constă în capitalul intelectual al cetățenilor. Progresul politic, social și economic din acest mileniu va depinde de potențialul intelectual al generațiilor de oameni tineri. Prin urmare, nu ar trebui să rămânem indiferenți la ceea ce învață elevii – cum anume învață și în ce mod trebuie să investească în competențele lor.

Lista competențelor necesare în secolul XXI reprezintă un model pentru învățământ, prin definiții adecvate și prin anumite contexte legate de cele mai necesare competențe ale elevilor. Pentru a fi pregătiți în mod adecvat, elevii trebuie să dobândească cunoștințe și competențe în cadrul contextului situațional contemporan. Transmiterea acestor competențe în era digitală și evaluarea corectă a competențelor deja dobândite de către elevi va determina dacă copiii de astăzi vor fi pregătiți să trăiască, să învețe, să muncească și să servească societății în mediul digital.

Starea actuală și cea viitoare a economiei mondiale și a fiecărui stat în parte depinde în mod direct de cât de bine va fi definit nivelul de alfabetizare în rândul persoanelor tinere. Aici vorbim de alfabetizarea secolului XXI, care include anumite competențe academice foarte dezvoltate, în ceea ce privește gândirea, înțelegerea, lucrul în echipă și utilizarea noilor tehnologii.

Pentru a progresa în economia digitală, elevii vor avea nevoie de anumite cunoștințe bazate pe era digitală. Elevii trebuie pregătiți pentru lumea din afara sălilor de clasă.

În opinia multora, lista celor mai importante competențe necesare pentru a avea succes în secolul XXI arată astfel:

ALFABETIZAREA ÎN ERA DIGITALĂ

În măsura în care societatea se schimbă, se schimbă și competențele necesare cetățenilor pentru a obține anumite lucruri complexe. La începutul secolului al XX-lea, era suficient ca o persoană să știe să scrie, să citească și să calculeze. Abia în urmă cu câțiva ani, sistemul de învățământ a început să ceară elevilor să citească în mod critic, să scrie convingător, să gândească logic și să rezolve probleme matematice și științifice complexe. Elevii trebuie, în primul rând, să dobândească alfabetizarea informatică și digitală. Alvin Toffler a afirmat că: „*Analfabetul*

secolului XXI nu va fi acela care nu poate citi sau scrie, ci acela care nu poate să învețe, să se dezvețe și să reînvețe. Cei care pot face acest lucru sunt liderii de mâine.”

- Alfabetizarea vizuală și informațională

Interfața grafică a Internetului și transferul vocii, a videourilor și a datelor în format digital au mărit drastic utilizarea instrumentelor vizuale. Tehnologiile avansate, precum camerele digitale, grafica, videoul și standardele de imagini, permit utilizarea imaginilor în scopul transmiterii de idei. Elevii au nevoie de competențe bune în ceea ce privește vizualizarea, pentru a putea să interpreteze imagini, pentru a observa anumite șabloane și pentru a putea să comunice prin intermediul imaginilor. Alfabetizarea informațională include accesul efectiv și eficient la informații, evaluarea informațiilor în mod critic și folosirea acestor informații în mod creativ și exact.

- Alfabetizarea culturală și conștientizarea globală

Lumea trăiește într-un ritm tot mai alert, iar odată cu globalizarea comerțului, a crescut și nevoia de alfabetizare culturală. Într-o astfel de economie globală, unde în întreaga lume, interacțiunea, parteneriatul și concurența se află în prim-plan, apare o necesitate din ce în ce mai crescută pentru cunoașterea, înțelegerea și respectul pentru alte culturi, inclusiv pentru cele care au fost stabilite drept norme în societatea tehnologică.

INVENTIVITATEA – CAPITALUL INTELECTUAL

- Adaptabilitatea/grija față de complexitate și autosesizarea

Legăturile care se stabilesc în lumea de astăzi manifestă o complexitate fără precedent. Globalizarea și Internetul sunt două noțiuni foarte complexe, care accelerează ritmul schimbărilor. Interacțiunile care au loc într-un astfel de mediu necesită ca indivizii să fie capabili să recunoască schimbările și să răspundă prompt la acestea – numai elevii care știu cum să recunoască schimbările pot să analizeze și să identifice condiții noi, precum și competențe noi de care vor avea nevoie pentru a face față condițiilor respective. De asemenea, elevii trebuie să fie capabili să aibă în vedere planuri de rezervă, trebuie să anticipeze schimbările și să înțeleagă legătura reciprocă dintre elementele din cadrul sistemului.

- Curiozitatea, creativitatea și riscul

De la angajatul viitorului, se așteaptă capacitatea de adaptare la un mediu în continuă schimbare. Pentru o astfel de învățare continuă, este necesară curiozitatea față de lumea înconjurătoare și față de modul în care aceasta funcționează. Curiozitatea asigură o învățare continuă, contribuind la o calitate mai bună a vieții și la capitalul intelectual al unui stat.

Aceeași importanță o are și asumarea riscului, fără de care nu ar fi existat multe dintre descoperirile, invențiile și cunoștințele pe care le știm astăzi.

- Gândirea și raționamentul la nivel înalt

Competențele de gândire sunt definite în felul următor: „*gândire creativă, luarea deciziilor, soluționarea problemelor, analiza lucrurilor și abilitatea de a ști să înveți.*” Raționamentul asigură elevilor planificarea, crearea, realizarea și evaluarea soluțiilor. Toate acestea sunt procese care, în cele mai frecvente cazuri, se aplică prin utilizarea instrumentelor tehnologice.

COLABORAREA

Colaborarea este un proces structurat, regenerabil, unde două sau mai multe persoane lucrează împreună pentru atingerea unui obiectiv comun. În cele mai frecvente cazuri, colaborarea este un efort intelectual de natură creativă – prin partajarea cunoștințelor, prin învățare și prin ajungerea la un consens. Colaborarea nu necesită leadership și poate conduce la rezultate mult mai bune prin descentralizare și egalitarism. Schimbările rapide din societatea de astăzi și rețelele de comunicare au provocat schimbări și la nivelul luării deciziilor. În același timp, complexitatea lumii contemporane necesită un nivel înalt de specializare a celor care iau decizii. De aici provine și nevoia de creare a unor echipe de specialiști care să fie responsabili cu efectuarea unor sarcini complexe. În acest sens, tehnologiile informaționale joacă un rol cheie atunci când este vorba de ușurința cu care are loc colaborarea între echipe și indivizi. E-mail-ul, fax-ul, mesageria vocală, conferințele audio și video, camerele de chat, documentele partajate și locurile de muncă virtuale pot asigura o colaborare reușită.

COOPERAREA

Cooperarea este un proces de lucru și acțiune comună, care se poate realiza cu ajutorul unor entități intenționate și neintenționate. În forma sa cea mai simplă, cooperarea pornește de la premisa că lucrurile trebuie să funcționeze în armonie, umăr la umăr, în timp ce în formele sale mai complexe, cooperarea se poate referi și la funcționarea ființei umane în cadrul social al unei națiuni. Aceasta este o alternativă la munca individuală, bazată pe competiție. Cooperarea se poate realiza, de asemenea, și cu ajutorul calculatorului, prin intermediul căruia se pot procesa simultan mai multe resurse comune în același timp.

Componentele individuale, care acționează independent, pot opera împreună pentru a crea un sistem mult mai complex și care poate avea o semnificație mult mai mare decât părțile sale individuale. Cooperarea poate fi impusă, voluntară sau chiar involuntară, motiv pentru care

indivizii și grupurile pot colabora, chiar și dacă nu au aproape nimic în comun în ceea ce privește interesele și obiectivele.

COMUNICAREA

Comunicarea este procesul care asigură indivizilor schimbul de informații cu ajutorul mai multor metode. Comunicarea este procesul prin care mesajul este trimis sau primit prin conversații, scriere sau gesturi.

Schimbul de informații necesită și un feedback, o reacție la ceea ce s-a transmis. Cuvântul *comunicare* este întrebuințat și în contextul în care există foarte puțin sau nu există deloc feedback, precum emiterea unui program, unde feedback-ul întârzie, deoarece emițătorul și receptorul utilizează metode, tehnologii, timp și moduri diferite de transmitere a informațiilor. Comunicarea se poate defini și ca un proces de interacțiune semantică între ființele umane. Acesta este un act de transmitere a informațiilor și un proces în care se schimbă sensuri pentru a ajunge la un anumit tip de înțelegere. Comunicarea implică trimiterea de mesaje, atât verbale, cât și nonverbale, fie că este vorba de o idee, un gest sau o acțiune stimulativă. Există mijloace auditive (vorbirea, intonația, ritmul etc.), precum și nonverbale (mimica, gestică, limbajul corporal, limbajul semnelor, contactul vizual sau scrisul). Comunicarea se desfășoară la mai multe niveluri și în moduri diferite. Există foarte multe definiții ale comunicării, dintre care unele recunosc faptul că animalele pot comunica între ele, dar și cu ființele umane, în timp ce alte definiții sunt mai restrânse și susțin faptul că comunicarea este o activitate preponderent umană. Cu toate acestea, există câteva elemente distincte care definesc comunicarea. Acestea sunt:

1. conținutul (ce se comunică);
2. sursa/emițătorul/expeditorul/cel care cifrează (cel care comunică);
3. forma (în ce formă se comunică);
4. canalul (prin ce mediu se comunică);
5. destinația/destinatarul/obiectivul/cel care descifrează (celui căruia i se comunică ceva);
6. sensul/aspectul pragmatic.

În societatea contemporană este necesar ca elevii să comunice prin utilizarea **tehnologiei**. Acest lucru include comunicarea sincronă și asincronă, precum e-mail-ul, interacțiunile în grup și locurile virtuale de învățare, camere chat, conferințe video interactive, telefon și interacțiuni prin stimuli și modele. Astfel de interacțiuni necesită cunoașterea conduitei tipice pentru un anumit mediu.

IT-ul nu schimbă ceea ce este necesar pentru o comunicare calitativă, însă oferă anumite dimensiuni noi, care trebuie învățate pentru a deveni transparente. În caz contrar, IT-ul va reprezenta mai degrabă un obstacol, decât o îmbunătățire a procesului de comunicare. Câteva noi dimensiuni, prezente în comunicarea globală, presupun programarea întâlnirilor și a ședințelor ținând cont de fusul orar, de culturile și limbile diferite.

CREATIVITATEA

Creativitatea este un proces mental care include generarea de noi idei sau concepte, sau generarea unor asocieri noi între idei și concepte deja existente. Din punct de vedere științific, produsele unei gândiri creative (uneori menționată ca gândire divergentă) sunt caracterizate prin originalitate. Ca alternativă, conceptul standard al creativității se referă la crearea a ceva nou.

Deși la prima vedere pare un fenomen intuitiv destul de simplu, creativitatea este în realitate mult mai complexă. Despre creativitate se spune că este har divin, o parte a procesului cognitiv sau un rezultat al mediului social și al trăsăturilor personale. Creativitatea este asociată cu genialitatea, cu bolile mintale sau cu umorul. Unii spun că este o trăsătură cu care ne naștem, pe când alții susțin că se poate învăța cu ajutorul unor tehnici simple.

Deși, în general, este legată de artă și literatură, creativitatea reprezintă o parte importantă a inovațiilor și a invențiilor și este importantă în profesii precum business-ul, economia, arhitectura, designul industrial, științele și ingineria.

ORGANIZAREA

Organizarea este un acord social care tinde spre atingerea unor obiective comune, care își controlează propriul efect și care are o limită ce îl delimitează de mediul înconjurător. Cuvântul organizare provine de la cuvântul grecesc „ὄργανον”, care înseamnă instrument.

SOLUȚIONAREA PROBLEMELOR

Soluționarea problemelor este o parte a procesului de gândire. Soluționarea problemelor este considerată drept cea mai complexă dintre toate funcțiile intelectuale, fiind definită ca un proces cognitiv de ordin superior, ce necesită modulație și un control de rutină al competențelor fundamentale.. Este parte a unui proces mai amplu, care include identificarea unei probleme și formularea acesteia.

AUTOSESIZAREA ȘI RESPONSABILITATEA SOCIALĂ

Tehnologiile de astăzi provoacă adesea dileme atunci când vine vorba de etică și valori. Datorită creșterii complexității tehnice, societatea noastră ar trebuie să ridice standardele etice și valorile la un nivel mai înalt, pentru a îndruma aplicarea științei și a tehnologiei în direcția corectă. Foarte important este ca elevii să înțeleagă această responsabilitate și, în calitate de cetățeni informați, să contribuie la aceasta pe toate planurile.

Elevii trebuie în primul rând să fie capabili de autoevaluare, monitorizare și înțelegere a propriilor nevoi, iar apoi trebuie să știe să localizeze resursele corespunzătoare și să transfere aptitudinile învățate dintr-un domeniu în altul.

De asemenea, comportamentul responsabil față de societate este la fel de important. Este necesară o armonie între comportamentul personal și interesul întregii comunități, precum și demonstrarea continuă a unui comportament etic pe plan personal, profesional și social.

CALITATEA, REZULTATELE ȘI PRODUCTIVITATEA EXCEPȚIONALĂ

Hank Levin a afirmat următoarele: *„Trebuie să fim foarte atenți atunci când vorbim despre standardele după care se creează o forță de muncă productivă pentru economie.”* Pe baza studiilor sale, Levin a ajuns la concluzia că niște rezultate bune la teste nu sunt în corelație cu productivitatea de la locul de muncă. Pe de altă parte, deși momentan nu se află în centrul atenției în școli, o înaltă productivitate determină dacă o persoană va avansa sau nu la locul de muncă.

- Prioritățile, planificarea și gestiunea având ca scop obținerea de rezultate

Un nivel înalt de complexitate necesită o planificare atentă și crearea planurilor de rezervă. Acestea sunt la fel de importante ca grija pentru rezultatele finale ale proiectului și concentrarea asupra atingerii obiectivelor principale. De asemenea, pentru a putea să anticipăm rezultatele neașteptate, este nevoie de flexibilitate și creativitate.

- Utilizarea efectivă a instrumentelor reale

A douăsprezecea regulă a lui Bill Gates referitoare la afaceri sună astfel: *„Utilizați instrumentele digitale pentru a-i ajuta pe clienți să-și rezolve singuri problemele.”* Această idee se bazează pe comunicare și networking. Alegerea instrumentelor adecvate și aplicarea lor în situații reale, astfel încât să obținem rezultatele cele mai bune, sunt, de asemenea, importante și pentru o mai bună colaborare, promovare și sporire a creativității.

- Rezultate de înaltă calitate aplicabile în mediul real

Cercetătorii văd un avantaj în tipul de învățare prin care elevii creează produse autentice, cu instrumentele corespunzătoare – fie că este vorba de un castel de nisip, programe de calculator,

documente, grafică, construcții LEGO sau compoziții muzicale. Astfel de experiențe oferă elevilor o perspectivă de ansamblu asupra oricărui domeniu ales.

ANEXA 3

COMPETENȚA DIGITALĂ

- ABILITATE ESENȚIALĂ PENTRU PROFESORI ȘI ELEVII ÎN SECOLUL XXI -

Competența digitală este esențială pentru educație, viață profesională și participare activă în societate. În cazul învățământului preuniversitar, este important să înțelegem această competență și, în egală măsură, să o cultivăm.

Ce este competența digitală?

Competența digitală este una dintre cele opt competențe-cheie, concretizându-se în utilizarea cu încredere și în mod critic a întregii game de tehnologii ale informației și comunicațiilor pentru informare, comunicare și soluționare a problemelor în toate domeniile vieții.

Un alt aspect care merită să fie luat în considerație este că „în calitate de competență transversală, competența digitală ne ajută să stăpânim și alte competențe-cheie, cum ar fi comunicarea, competențele lingvistice sau cele de bază în matematică și științe”. (Dr Riina Vuorikari – “*Dobândirea competenței digitale – misiunea cetățenilor secolului 21*”)

Pentru a înțelege mai bine natura acestei competențe, Comisia Europeană a conceput *Cadrul european al competenței digitale pentru cetățeni* (DigComp), structurat în cinci domenii: alfabetizarea digitală și informațională, comunicare și colaborare, creare de conținut digital, siguranță și soluționare de probleme.

Cum este promovată dezvoltarea competenței digitale în Europa?

Raportul Eurydice arată că aproape toate țările europene au o strategie națională vizând competența digitală. La momentul realizării studiului, competența digitală era predată, prin intermediul unei abordări interdisciplinare, în învățământul primar din aproape toate țările UE și în învățământul secundar din toate țările, în paralel cu alte abordări folosite în unele țări, precum integrarea TIC în anumite discipline sau predarea acestuia ca disciplină separată.

Unul dintre factorii-cheie este asigurarea unui nivel suficient de competență digitală în rândul profesorilor. Cea mai mare rețea a profesorilor din Europa, **eTwinning**, oferă profesorilor un mediu ideal pentru a colabora cu colegii și a descoperi modalități noi de utilizarea a TIC în predare. eTwinning a avut un impact important asupra abilității profesorilor de a folosi

tehnologiile în predare. eTwinner-ii au semnalat și o creștere a gradului de utilizare a practicilor de predare-învățare digitale.

“Dobândirea competenței digitale – misiunea cetățenilor secolului 21”

Dr Riina Vuorikari

Munca, capacitatea de inserție profesională, educația, timpul liber, incluziunea și participarea la societate, toate acestea și multe alte domenii ale societății noastre sunt tot mai „digitizate”: informația și serviciile sunt mai des oferite prin intermediul Internetului. Ca urmare, competența digitală este esențială pentru participarea la economia și societatea actuală. Fiind o competență transversală, competența digitală ne ajută să stăpânim și alte competențe-cheie, cum ar fi comunicarea, competențele lingvistice sau cele de bază în matematică și științe.

A fi competent digital în lumea de astăzi nu presupune doar accesul și utilizarea tehnologiilor informației și comunicării, ci și cunoștințe, abilități și atitudini adecvate față de acestea. Conform unui studiu asupra incluziunii și competențelor digitale în UE, 50% din populația UE posedă o competență digitală insuficientă. Dintre aceștia, jumătate posedă o competență zero.

Competența digitală nu presupune doar să știi cum să navighezi pe Internet. Ea poate fi defalcată într-o serie de componente mai mici. Cadrul european al competenței digitale pentru cetățeni, cunoscut și sub denumirea de DIGCOMP, conturează cinci domenii care definesc cetățeanul „competent digital”: procesarea informației, comunicarea, crearea de conținut, siguranța și soluționarea problemelor. În curând, cetățenii UE vor beneficia de un instrument online de evaluare, care le va facilita accesul rapid și simplu la competența lor digitală. Începând din vara lui 2015, persoanele aflate în căutarea unui loc de muncă folosesc instrumentul de evaluare a competenței digitale în cadrul CV-ului Europass, ceea ce le permite să menționeze nivelul de competență digitală direct în CV.

DIGCOMP este utilizat și de factorii de decizie politici, și de autoritățile educaționale. Recent lansatul Index paneuropean al societății și economiei digitale folosește cadrul DIGCOMP pentru a elabora un indicator ce oferă informații privind situația competenței digitale a cetățenilor fiecărei țări membre. Cadrul servește și la planificarea și proiectarea de oferte de educație și formare, de exemplu ca bază de plecare pentru revizuirea programelor școlare, pentru proiectarea cursurilor destinate educației adulților și pentru proiectarea programelor de dezvoltare profesională a profesorilor. De asemenea, servește și la definirea nivelului de competență digitală din diverse sectoare, cum ar fi, de exemplu, cel al asistenței sociale.

La capitolul competenței digitale a profesorilor, studiile din domeniu au subliniat în mod repetat lipsa de oportunități de formare profesională, cu precădere din domeniul utilizării TIC în scopuri pedagogice. De asemenea, se înregistrează un deficit de oportunități de perfecționare a competențelor TIC, astfel încât orice ocazia de a participa la activități de formare informale poate fi în avantajul profesorilor. De exemplu, **eTwinning** pune la dispoziția profesorilor o rețea de colaborare profesională, care poate contribui la însușirea unor noi strategii didactice de lucru cu TIC sau la stimularea sentimentului eficacității personale. Publicația *Rețelele de profesori* oferă puncte de vedere și date despre provocările și oportunitățile profesiei de cadru didactic. În mod similar, **eTwinning** poate contribui la dezvoltarea competențelor elevilor, inclusiv a celor digitale.

ANEXA 4

STANDARDE DE COMPETENȚĂ DIGITALĂ PENTRU CADRELE DIDACTICE DIN ȘCOALĂ

Competențele digitale reprezintă ansambluri dinamice de cunoștințe, abilități, deprinderi, atitudini și valori, formate și dezvoltate prin învățare, pe care le posedă un individ și care pot fi mobilizate pentru a soluționa diverse probleme ce apar în procesul colectării, păstrării, prelucrării și diseminării informației prin intermediul tehnologiilor informației și a comunicațiilor.

Pe măsură ce tehnologiile sunt integrate în toate activitățile din orice domeniu, capacitatea de a utiliza aceste tehnologii și de a ține pasul cu evoluția lor rapidă a devenit o condiție obligatorie întrucât tehnologiile digitale transformă fiecare aspect al vieții, de la stilul de viață personal la activitatea de la locul de muncă.

În secolul XXI profesorii trebuie să posede competențe digitale pentru a face față provocărilor erei informaționale. Necesitatea deținerii unui anumit nivel de competențe digitale are două fațete pentru profesori: parte integrantă a competențelor profesionale; stimulent și catalizator pentru dezvoltarea competențelor digitale ale elevilor ca prerogativă de angajare a acestora în câmpul muncii.

Competențe digitale strict necesare unui cadru didactic pentru a realiza activitățile profesionale:

- acces la cele mai bune resurse și conținuturi educaționale;
- comunicare cu colegii, părinții și în cadrul rețelelor profesionale;
- efectuarea managementului activităților didactice prin instrumente digitale.

Domeniul TIC este unul foarte dinamic, viteza de dezvoltare a noilor instrumente și oportunități fiind foarte mare, iar gama și complexitatea competențelor necesare pentru a fi pedagog în secolul XXI este atât de mare încât cadrele didactice trebuie să-și actualizeze în mod constant competențele și să le adapteze, iar acest lucru necesită atitudini critice bazate pe dovezi, care să le permită să fie responsabili de rezultatele elevilor

COMPETENȚE DIGITALE PENTRU CADRELE DIDACTICE

Domeniile de competență digitală:

1. Comunicarea digitală
2. Gestionarea informației
3. Crearea de conținuturi digitale educaționale
4. Implementarea aplicațiilor de management școlar
5. Sisteme de gestionare a conținuturilor educaționale (SGCE)
6. Utilizarea echipamentelor digitale în educație
7. Respectarea normelor etice și legale în spațiul digital

Domeniile de competență digitală		
Nivel de bază	Nivel intermediar	Nivel avansat
1. Comunicare digitală		
Utilizează instrumentele standard de comunicare pentru transmiterea și recepționarea sarcinilor de învățare, feed-back individual și de grup etc.	Utilizează instrumentele avansate de comunicare pentru realizarea diferitor activități de învățare;	Activează într-un mediu de comunicare, digital; Realizează diverse activități educaționale nemijlocit în mediul digital;
Este membru al grupurilor / comunităților profesionale virtuale, urmărește activitatea grupului, noutățile și problemele discutate, fără a se implica în conversații	Este membru al comunităților profesionale virtuale, participă în activitatea grupului, pune în discuție noutăți și probleme,	Este creator/membru al grupurilor/comunităților profesionale virtuale, gestionează activitatea grupului, dezvoltă și promovează activitatea acestuia în Rețea.
2. Gestionarea informației		
Utilizează tehnici standard pentru a identifica resursele digitale în Rețea;	Utilizează tehnici avansate de căutare în Rețea;	Dezvoltă mediul informațional digital propriu, din care selectează resurse relevante folosind o multitudine de metode
Organizează datele în fișiere și directoare în medii locale și externe	Gestionează drepturile de acces la date în medii locale și externe	Organizează prelucrarea în comun a datelor la distanță

Cunoaște criteriile de evaluare a validității informației	Aplică criteriile de evaluare a validității informației	Adaptează criteriile de evaluare a validității informatice la contextele didactice
3. Crearea de conținuturi digitale educaționale		
Utilizează resurse digitale disponibile-existente în procesul didactic	Îmbunătățește resursele existente prin aplicarea opțiunilor avansate ale aplicațiilor generice	Crează resurse digitale proprii. Integrează dinamic text, date, obiecte multimedia proprii sau preluate din locații externe în resursele utilizate în dependență de necesitate
Evaluează calitatea resurselor digitale utilizând criterii prestabilite	Analizează critic calitatea resurselor digitale prin compararea cu alte resurse, corelarea cu necesitățile educaționale, stabilirea și evaluarea criteriilor de evaluare	Analizează critic calitatea resurselor digitale prin îmbinarea unor criterii complexe. Propune și realizează în colaborare îmbunătățiri
Informează cadrele didactice despre resursele digitale disponibile	Promovează utilizarea resurselor digitale în mediul pedagogic	Realizează sesiuni de training pentru colegi și alte grupuri țintă în vederea utilizării TIC în procesul didactic
Încurajează elevii să prezinte rezultatele învățării în format digital	Implică elevii în evaluarea și editarea resurselor digitale produse de colegi	Implică elevii în crearea resurselor digitale
Identifică softuri educaționale relevante pentru a le utiliza în disciplinele, pe care le predă.	Integrează softuri educaționale în procesul didactic în mod adecvat	Contribuie la elaborarea scenariilor și elaborarea softurilor educaționale
4. Implementarea aplicațiilor de management școlar		
Utilizează sistemele de management școlar pentru activități de planificare	Promovează utilizarea sistemelor de management școlar pentru activități de planificare	Realizează sesiuni de training pentru colegi și alte grupuri țintă în vederea utilizării sistemelor de management școlar
Utilizează sistemele de management școlar pentru comunicare	Promovează utilizarea sistemelor de management școlar pentru comunicare	Realizează sesiuni de training pentru grupuri țintă în vederea utilizării sistemelor de management școlar pentru comunicare

Utilizează aplicații de management școlar pentru gestionarea procesului de evaluare	Promovează avantajele aplicațiilor de management școlar pentru gestionarea procesului de evaluare	Utilizează instrumentele de analiză statistică integrate în aplicațiile de management școlar pentru analiza progresului elevilor
Utilizează sistemele de gestiune a clasei digitale pentru monitorizarea elevilor și grupurilor pe parcursul activităților educaționale	Coordonează activitatea elevilor pe parcursul activităților educaționale prin intermediul clasei digitale	Configurează sistemele de gestiune a clasei digitale în funcție de specificul clasei
5. Sisteme de gestionare a conținuturilor educaționale (SGCE)		
Utilizează resurse educaționale digitale din SGCE	Adaptează / actualizează resursele educaționale existente pentru utilizare în cadrul SGCE	Integrează în SGSA resurse educaționale proprii conform unor scenarii elaborate anterior, folosind instrumentele creative ale sistemului , alte softuri specializate pentru crearea și dezvoltarea resurselor digitale
Utilizează resurse pentru evaluare, din SGCE	Adaptează / actualizează resurse pentru evaluare locală în cadrul aplicațiilor de evaluare, integrate în SGCE	Creează și gestionează resurse pentru evaluare locală în cadrul aplicațiilor de evaluare, integrate în SGCE
Utilizează resursele sistemelor de gestionare a conținuturilor pentru realizarea activităților educaționale cu grupuri de elevi în cadrul unei clase	Individualizează la nivel de elev sarcinile de învățare prin mixarea resurselor integrate în SGCE	Elaborează parcursuri individuale de învățare pentru elevi sau grupuri de elevi prin mixarea resurselor integrate în SGCE și utilizarea resurselor proprii
6. Utilizarea echipamentelor digitale în educație		
Utilizează funcționalitățile de bază ale echipamentelor digitale de uz general pentru activități de instruire și comunicare în instituție	Utilizează funcționalitățile avansate ale echipamentelor digitale de uz general pentru activități de instruire și comunicare în instituție	Identifică și experimentează noi modele de utilizare a echipamentelor digitale de uz general și a celor specializate pentru organizarea creativă a activităților educaționale

Utilizează funcționalitățile de bază ale tablei interactive	Utilizează funcționalitățile avansate ale tablei interactive	Utilizează echipamente specializate : laboratorul virtual, microscopul digital; seturi digitale integrate pentru studierea limbilor străine
Utilizează funcționalitățile de bază ale dispozitivelor digitale multimedia în producerea resurselor digitale multimedia cu caracter educațional	Utilizează funcționalitățile avansate ale dispozitivelor digitale multimedia în producerea resurselor digitale multimedia cu caracter educațional	Instruiește grupuri țintă în utilizarea dispozitivelor digitale multimedia în producerea resurselor digitale multimedia cu caracter educațional
Identifică problemele tehnice apărute în procesul de utilizare a echipamentelor	Describe specificul problemelor tehnice apărute în procesul de utilizare a echipamentului și apelează la suport tehnic specializat	Contribuie la soluționarea problemelor tehnice de utilizare a echipamentului (în cazul în care soluția nu implică riscuri de sănătate sau alte riscuri)
7. Respectarea normelor etice și legale în spațiul digital		
Utilizează rațional din punct de vedere energetic dispozitivele electronice	Identifică efectele pozitive și negative ale tehnologiilor informaționale asupra mediului înconjurător și sănătății umane	Ia decizii informate referitor la dispozitivele electronice pe care le procură și modul în care le utilizează, ținând cont de impactul acestora asupra mediului înconjurător și sănătății umane
Utilizează instrumentele de securitate cibernetă prestabilite pentru protecția datelor și echipamentelor în mediul digital personal (antivirus, firewall, parole)	Variază strategiile de securitate pe care le utilizează(antivirus, firewall, parole); Identifică amenințările de securitate și apelează la ajutor pentru a le înlătura	Configurează aplicațiile de securitate cibernetă pe care le deține; Rezolvă amenințările de securitate cu care se confruntă
Explică riscurile asociate distribuirii informațiilor cu caracter personal pe internet	Utilizează instrumente care asigură confidențialitatea informațiilor cu caracter personal pe internet	Ia decizii cu privire la aplicațiile și circumstanțele în care i se colectează date cu caracter personal

Explică elevilor și colegilor fenomenul de agresiune cibernetică	Informează organele abilitate în cazul depistării situațiilor de agresiune cibernetică	Întreprinde activități de prevenire a cazurilor de agresiune cibernetică
Respectă regulile de utilizare a resurselor digitale în distribuție liberă și a celor proprietare	Explică elevilor și colegilor regulile de utilizare a resurselor digitale în distribuție liberă și a celor proprietare	Promovează regulile de utilizare a resurselor digitale în distribuție liberă și a celor proprietare
Utilizează instrumente prestabilite de depistare a plagiatului	Selectează instrumente pentru depistarea plagiatului	Promovează instrumentele pentru depistarea plagiatului
Cunoaște prevederile legislației în domeniul protecției copiilor în mediul digital, educația digitală, infracțiunile cibernetice, protecția datelor, etc.	Explică prevederile legislației în domeniul protecției copiilor în mediul digital, educația digitală, infracțiunile cibernetice, protecția datelor, etc.	Promovează prevederile legislației în domeniul protecției copiilor în mediul digital, educația digitală, infracțiunile cibernetice, protecția datelor, etc.