



Colegiul Economic
"Mihail Kogălniceanu"
Focșani



Inspectoratul
Școlar Județean
Vrancea



MINISTERUL
EDUCAȚIEI

REGULAMENT

PRIVIND SIGURANȚA ONLINE ȘI UTILIZAREA
DISPOZITIVELOR ELECTRONICE LA
COLEGIUL ECONOMIC
"MIHAIL KOGĂLNICEANU" FOCȘANI

2024



REGULAMENT

PRIVIND SIGURANȚA ONLINE ȘI UTILIZAREA

DISPOZITIVELOR ELECTRONICE LA

COLEGIUL ECONOMIC "MIHAIL KOGĂLNICEANU" FOCȘANI

Nr. 1675/12.09.2024

Lista responsabililor cu elaborarea/revizuirea, verificarea și aprobarea **Regulamentului privind siguranța online și utilizarea dispozitivelor electronice la Colegiul Economic "Mihail Kogălniceanu" Focșani**

Elemente privind responsabilii/Operațiunea	Numele și prenumele	Funcția	Data	Semnătura
Elaborat	Prof. Vișan Carmen Corina	Profesor, aria curriculară Tehnologii	04.09.2019	
Revizuit 1	Prof. Vișan Carmen Corina	Profesor, aria curriculară Tehnologii	16.09.2022	
Revizuit 2	Prof. Vișan Carmen Corina	Profesor, aria curriculară Tehnologii	12.09.2024	
Verificat	Prof. Tudor Mihaela	Director adjunct, Colegiul Economic "Mihail Kogălniceanu" Focșani	12.09.2024	
Aprobat	Prof. Bocsok Gabriela Dorina	Director, Colegiul Economic "Mihail Kogălniceanu" Focșani	12.09.2024	



CUPRINS

I. INTRODUCERE	4
II. UTILIZAREA ACCEPTABILĂ A POLITICII DE TEHNOLOGIE A INFORMAȚIEI ȘI A COMUNICĂRII	5
2.1. Tipuri de instrumente.....	6
2.2. Obligațiile utilizatorilor.....	7
2.3. Obligațiile profesorilor	8
2.4. Obligațiile elevilor	9
2.5. Ghid pentru curățarea și dezinfectarea zonei de lucru și a dispozitivelor electronice	11
III. UTILIZAREA ALTOR ECHIPAMENTE ELECTRONICE OFERITE DE COLEGIUL ECONOMIC "MIHAIL KOGĂLNICEANU" FOCȘANI.....	13
IV. ECHIPAMENTE PERSONALE.....	14
V. PUBLICAREA CONȚINUTULUI	16
VI. ACȚIUNEA ÎN CAZ DE INCIDENTE	17
VII. CYBERBULLYING	18
VIII. SUPERVIZARE	21
IX. DIVULGAREA DATELOR.....	23
X. BIBLIOGRAFIE	25
XI. ANEXE.....	26
11.1. Fișa informațională nr. 1 – Conectarea	26
11.2. Fișa informațională nr. 2 – Crearea paginilor web	29
11.3. Fișa informațională nr. 3 – Căutarea informației	34
11.4. Fișa informațională nr. 4 – Poșta electronică.....	37
11.5. Fișa informațională nr. 5 – Chat-urile.....	41
11.6. Fișa informațională nr. 6 – Muzica și imaginile pe Internet.....	47
11.7. Fișa informațională nr. 7 – Viața privată.....	51
11.8. Fișa informațională nr. 8 – Securitatea	56
11.9. Fișa informațională nr. 9 – Intimidarea și hărțuirea	59
11.10. Fișa informațională nr. 10 – Tehnologia mobilă.....	62
11.11. Formularul de consimțământ privind utilizarea Internetului la Colegiul Economic "Mihail Kogălniceanu" Focșani	66

I. INTRODUCERE

Politicile de securitate electronică a școlii s-au dezvoltat rapid, deoarece tehnologiile digitale sunt parte a vieții noastre de zi cu zi. Pentru a ne asigura că utilizarea eMedia este realizată în cel mai sigur mod posibil, indiferent dacă elevii sunt acasă, la școală sau în timpul liber, cu prietenii sau singuri, Colegiul Economic "Mihail Kogălniceanu" Focșani are o politică școlară clară și concisă care acordă atenție tuturor aspectelor privind siguranța pe Internet / eSafety.

Copiii, tinerii și adulții interacționează permanent cu tehnologiile informației și comunicațiilor, cum ar fi computere, laptop-uri, tablete, telefoane mobile... printr-o conexiune continuă la Internet, iar utilizarea lor este văzută ca un instrument de învățare. Acțiunea tehnologiei în mediul social a crescut rapid în rândul oamenilor și servește ca o completare a utilizatorilor în căutarea informațiilor și a cunoștințelor, prezentând astfel beneficii enorme. Cu toate acestea, atunci când sistemul informațional electronic este utilizat necorespunzător, poate duce la situații de risc.

Acest document, care stabilește regulile de utilizare acceptabilă a tehnologiilor informaționale și de comunicare, și are ca scop reglementarea utilizării echipamentelor și infrastructurilor disponibile, a fost elaborat cu scopul de a informa utilizatorii despre regulile și procedurile care reglementează utilizarea lor în grup, de către elevii, profesorii și personalul de la Colegiul Economic "Mihail Kogălniceanu" Focșani.

Regulile și procedurile s-au bazat pe orientările legale actuale și vizează utilizarea rațională și conștientă a acestor resurse și servicii, precum și păstrarea și integritatea datelor utilizatorilor.

Stimați utilizatori, siguranța dumneavoastră online este prioritatea politicii noastre ca instituție de învățământ!

II.UTILIZAREA ACCEPTABILĂ A POLITICII DE TEHNOLOGIE A INFORMAȚIEI ȘI A COMUNICĂRII

Ultimele două decenii au transformat tehnologia informației și comunicării (TIC) dintr-un produs destinat unui număr restrâns de indivizi, datorită costurilor ridicate de achiziție și a dimensiunilor relativ mari, într-un instrument omniprezent în viața profesională și personală a oamenilor. Avantajele TIC nu sunt deloc neglijabile, fapt care a atras răspândirea rapidă în activități educaționale, fie ele formale sau non-formale.

Educația s-a folosit de oportunitatea oferită de TIC pentru a-și regândi modalitatea de furnizare a conținuturilor educaționale, într-o manieră care să îmbunătățească performanțele elevilor, fără costuri excesive pentru sistem.

Managementul beneficiarilor serviciilor educative poate fi îmbunătățit prin crearea de instrumente care să urmărească progresele obținute atât de fiecare individ în parte, cât și de grupuri mai mari. Indiferent că vorbim de grupuri care există în realitate (ex. o clasă de elevi) sau de unele construite în mod convențional (ex. elevi din mediul rural), bazele de date și instrumentele de procesare a informației ne permit să urmărim cu ușurință dinamica apărute și să intervenim în caz că am considera oportun să aducem o schimbare.

Unul dintre cele mai vizibile beneficii pe care le aduce TIC este accesibilitatea informației. Ceea ce până de curând putea fi consultat doar de grupuri restrânse, astăzi a devenit accesibil unui număr teoretic nelimitat de oameni. Creatorul informației este liber să limiteze răspândirea ei către anumite grupuri, dar, de asemenea, are la dispoziție instrumente prin care să o propage către persoanele potențial interesate.

Prin intermediul noilor tehnologii se urmărește și promovarea autonomiei utilizatorilor, care sunt încurajați să se folosească de instrumentele puse la dispoziție pentru a-și planifica și monitoriza parcursul educațional și de carieră.

Instrumentele TIC favorizează construirea unor practici bazate pe probe și feedback, fapt ce este de natură să crească nivelul serviciilor educaționale prin introducerea unui „cerc al calității” (proiectare, implementare, evaluare și revizuirea activităților).

2.1. Tipuri de instrumente

Bazele de date sunt instrumente prin care se colectează și se organizează informații despre anumite subiecte pentru a facilita accesul persoanelor interesate. În mediul educațional, bazele de date se pot referi atât la unele generate de instituții prin efort colectiv (ex. profile ocupaționale), cât și la cele create de profesori (ex. fișele beneficiarilor). Deși bazele de date au existat cu mult timp înainte de apariția tehnologiilor digitale, doar odată cu introducerea acestora s-a atins un nivel de accesibilitate și eficiență care să conducă la generalizarea utilizării lor.

Cu o largă răspândire chiar și înainte de era Internetului, **instrumentele de procesare a informației** (audio, video, imagini, text) fac parte din programele cele mai întrebuintate, atât de către utilizatorii profesionali cât și de cei cu scop recreativ. Ele permit crearea de noi conținuturi sau rearanjarea unora deja existente.

Rețelele de socializare online sunt aplicații care facilitează întâlnirea în spațiul virtual a unor persoane care de obicei împărtășesc interese comune. Răspândite începând cu primul deceniu al secolului XXI, ele au devenit foarte repede fenomene de masă. Într-un timp relativ scurt cele mai mari rețele au atins sute de milioane de utilizatori și continuă să se dezvolte în ciuda controverselor care le-au însoțit expansiunea.

Rețelele profesionale sunt o variantă particulară a rețelilor de socializare, care se concentrează pe aspecte ce țin de un anumit domeniu de activitate. Existența lor poate fi susținută de o platformă dedicată (ex. LinkedIn, Yammer) sau prin adaptarea unui serviciu cu caracter general (ex. listă discuții).

Instrumentele de promovare și autopromovare au o valoare specială în cadrul activităților de consiliere de carieră întrucât, prin intermediul lor, elevul poate fi abilitat să-și gestioneze relația cu potențialii angajatori. Scopul lor este de a facilita relația dintre angajator și potențialul angajat prin punerea informației într-o formă ușor accesibilă și care scoate în evidență calitățile celui care caută un loc de muncă.

Instrumentele de comunicare, simple sau complexe, sincrone sau asincrone, gratuite sau plătite, sunt unele dintre cele mai apreciate facilități oferite de noile tehnologii. Ele au

revoluționat modul de comunicare prin reducerea dramatică a costurilor și disponibilitatea lor în aproape orice colț al lumii.

Instrumentele de evaluare și autoevaluare a serviciilor oferite sunt percepute ca unul dintre cele mai utile instrumente pentru consiliere și orientare pe care TIC le-a adus. Ușurința cu care ele pot fi dezvoltate, costurile relativ scăzute de a le aplica și interpretarea lor aproape instantanee le-au transformat din niște instrumente greoaie, care necesitau multe ore de muncă pentru a scoate informația relevantă, în maniera predilectă de a porni sau monitoriza procesul de consiliere și orientare.

2.2. Obligațiile utilizatorilor

1. Utilizați în mod corespunzător sistemele de informații ale Colegiului Economic "Mihail Kogălniceanu" Focșani, știind că, în conformitate cu legislația din România și directivele Europene, următoarele acte constituie o infracțiune, care se pedepsește prin lege:

- obținerea accesului neautorizat la materialele informatice;
- obținerea accesului neautorizat la materiale informatice pentru a comite sau a facilita alte acte ilegale sau pentru a schimba materialele informatice fără autorizație.

2. Utilizați toate echipamentele și programele informatice furnizate de Colegiul Economic "Mihail Kogălniceanu" Focșani pentru activitatea utilizatorilor săi, numai în scopuri legate de școală, fără acces la sisteme sau date personale.

3. Închideți întotdeauna sesiunea de lucru sau echipamentul pe care tocmai l-ați utilizat, eliminând toată documentația produsă de pe Desktop și din folderul „Documente”, apoi golind coșul de gunoi / Recycle Bin.

4. Respectați sistemul de securitate și nu dezvăluiți nicio parolă sau informații de securitate.

5. Asigurați-vă că datele personale ale elevilor, profesorilor sau părinților / tutorilor sunt protejate în conformitate cu legislația națională, în special în ceea ce privește modul în care sunt obținute, prelucrate, întreținute, transferate, accesate și utilizate.

6. Folosiți fotografiile și / sau videoclipuri ale elevilor minori numai după ce ați obținut acordul părinților /tutorilor legali.
7. Nu stocați fișiere digitale profesionale, care conțin informații personale sau sensibile, legate de Colegiul Economic "Mihail Kogălniceanu" Focșani (inclusiv documente, imagini, videoclipuri etc.) pe orice dispozitiv personal (cum ar fi: laptop-uri, CD, camere digitale, telefoane mobile), cu excepția cazului în care sunt stocate în mod corespunzător, sunt protejate împotriva accesului neautorizat, a furtului și a utilizării frauduloase.
8. Nu stocați, în sistemul informatic și în OneDrive, informații / date personale care nu au legătură cu activitățile școlare.
9. Respectați drepturile de proprietate intelectuală.
10. Nu este permisă instalarea nici unui program, fără autorizația administratorului de sistem.
11. Raportați directorului Colegiului Economic "Mihail Kogălniceanu" Focșani orice incident îngrijorător în ceea ce privește siguranța elevilor în utilizarea TIC / tehnologiilor informaționale și de comunicare, orice activitate suspectată pe un dispozitiv sau sistem și orice pierdere de fișier digital sau informații legate de viruși informatici.
12. **Este interzis** să creați, să prezentați, să publicați sau să transmiteți materiale prin care puteți hărțui, jigni, provoca neplăceri sau anxietate inutile unei persoane sau care poate discredita Colegiul Economic "Mihail Kogălniceanu" Focșani, sistemul educațional sau comunitatea locală.

2.3. Obligațiile profesorilor

1. Să fie responsabil în ceea ce privește controlul și utilizarea corectă a echipamentelor și programelor informatice în timpul orei.
2. Informarea elevilor cu privire la regulile care trebuie respectate în laboratoarele de informatică / AEL și cabinetele metodice la utilizarea sistemului informatic.
3. Supraveghează elevii în clasă, în laboratoare și în alte spații școlare.

4. Verifică echipamentul / software-ul calculatorului și înregistrează orice anomalii în documentul „Jurnalul de defecțiuni al echipamentului calculatorului”, care este prezentat administratorului de sistem.
5. Promovează securitatea digitală în rândul elevilor, ajutându-i să dezvolte o atitudine responsabilă atunci când accesează Internetul, folosind sisteme informatice și conținutul pe care îl creează și îl vizualizează.
6. După utilizarea laboratoarelor de informatică / AEL, cabinetelor metodice, trebuie să aibă în vedere următoarele:
 - a. calculatoarele sunt închise;
 - b. scaunele sunt așezate în ordine;
 - c. mesele sunt curate;
 - d. spațiul este organizat și curat.

2.4. Obligațiile elevilor

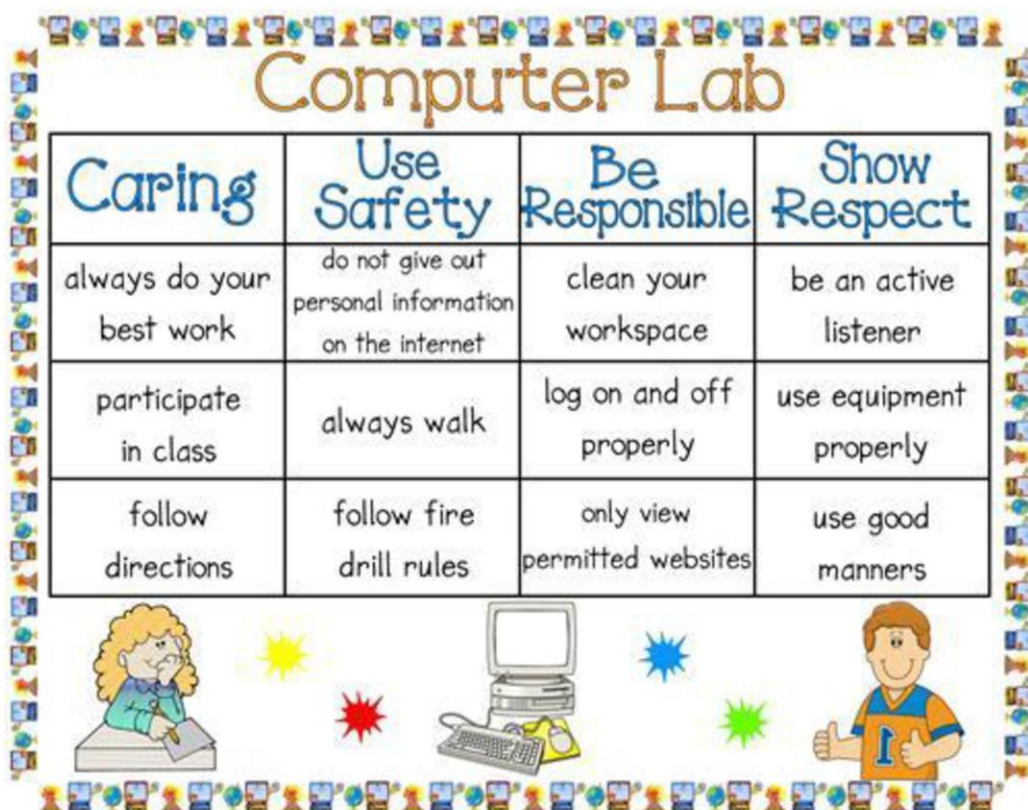
1. Să pornească calculatorul și să-l oprească corect și să raporteze defecțiunile în timpul utilizării.
2. Execută **numai** sarcinile indicate de profesor, respectând toate regulile de funcționare ale laboratorului de informatică / AEL, cabinetului metodic.
3. Să fie responsabil de realizarea copiilor / înregistrărilor privind documentele / lucrărilor executate.
4. Să se asigure că activitatea online respectă și nu jignește comunitatea școlară.
5. Să aibă grijă de curățenia clasei, lăsând locul curat și ordonat.

Este strict interzis:

1. Să modifice setările inițiale ale sistemului de operare. Dacă elevii vor face acest lucru, ei vor fi responsabili pentru pagubele pe care le-ar putea provoca, și vor răspunde material pentru acoperirea prejudiciului.

2. Să schimbe parola de acces.
3. Să contribuie la distrugerea vreunui echipament sau software sau să modifice conexiunile existente.
4. Să descarce / să copieze jocuri, videoclipuri, imagini sau muzică care nu fac parte din program.
5. Să intre în laboratorul de informatică / AEL, cabinetul metodic în absența unui profesor, decât dacă este autorizat de director / director adjunct / administratorul de sistem.

Elevii trebuie să înțeleagă că regulile au fost create pentru siguranța lor și că vor fi trași la răspundere și sancționați în caz de nespectare / încălcare a prevederilor.



2.5. Ghid pentru curățarea și dezinfectarea zonei de lucru și a dispozitivelor electronice

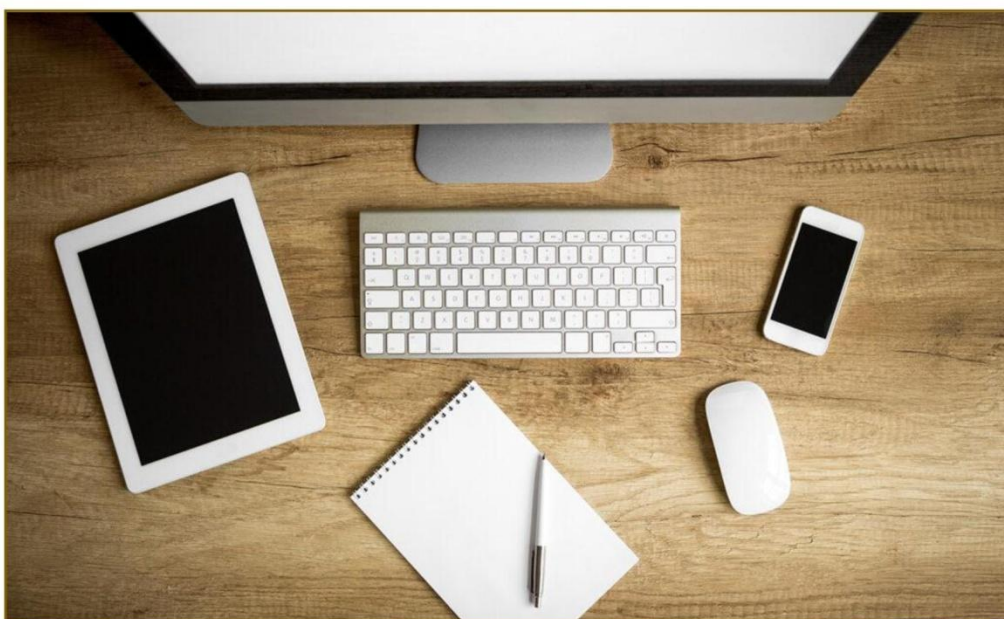
Pandemia cauzată de virusul SARS-COV2 impune măsuri suplimentare de protecție privind igienizarea mâinilor, purtarea măștii de protecție, dezinfectarea suprafețelor de lucru și a dispozitivelor electronice.

Pentru curățarea și dezinfectarea zonei de lucru se recomandă folosirea cârpelor sau a prosoapelor de microfibră – încearcă să eviți folosirea bureților care ar putea zgâria suprafețele – și a unui produs dezinfectant neabraziv, adică, fără clor.

Înainte de curățare, trebuie să închizi și să scoți din priză dispozitivele, să le scoți bateriile detașabile și să aștepți câteva minute până când se răcesc. Iată cum trebuie să dezinfectezi suprafețele, obiectele și dispozitivele din zona de lucru:

- **Birou:** curăță masa cu o cârpă umedă și un produs dezinfectant. Pulverizează direct pe suprafață la o distanță de 20 cm și șterge toată suprafața cu o cârpă curată și umedă.
- **Scaun:** pentru curățarea și dezinfectarea scaunului trebuie să ții cont de materialul din care este fabricat. În cazul în care este un scaun din piele, poți folosi cârpa cu produsul dezinfectant. Dar dacă este tapițat cu material textil, este preferabil să fie curățat cu apă și detergent sau cu un dezinfectant specific.
- **Telefon mobil sau tabletă:** pulverizează substanța dezinfectantă pe o cârpă curată puțin umezită, niciodată direct pe dispozitive. Poți folosi de asemenea un șervețel dezinfectant multi-suprafețe.
- **Calculator:** trebuie să cureți și să dezinfectezi zonele pe care le atingi mai frecvent, ca de exemplu butonul de pornire. Ai grijă cu conectoarele precum cele USB.
 - ✓ **Tastatură:** pentru curățarea suprafeței tastaturii, îți recomandăm să o ștergi cu o cârpă umezită sau un șervețel dezinfectant universal.
 - ✓ **Mouse:** trebuie să insiști în zonele care intră în contact cu mâinile sau degetele. Dacă folosești un suport pentru deplasarea mouse-ului, trebuie de asemenea șters cu o cârpă umezită cu lichid dezinfectant.

- ✓ **Ecran:** curăță zona externă – margini și butoane. Pentru ecran, poți folosi o cârpă uscată și un produs specific pentru această suprafață.
- **Căști:** dacă te numeri printre cei care ascultă muzică la căști în timp ce lucrează, este de asemenea foarte important să le dezinfectezi. Folosește o cârpă de microfibră cu dezinfectant.
- **Dispozitive USB** (memorii USB, discuri dure portabile,...) **și încărcătoare:** folosește o cârpă umedă fără să atingi partea metalică.



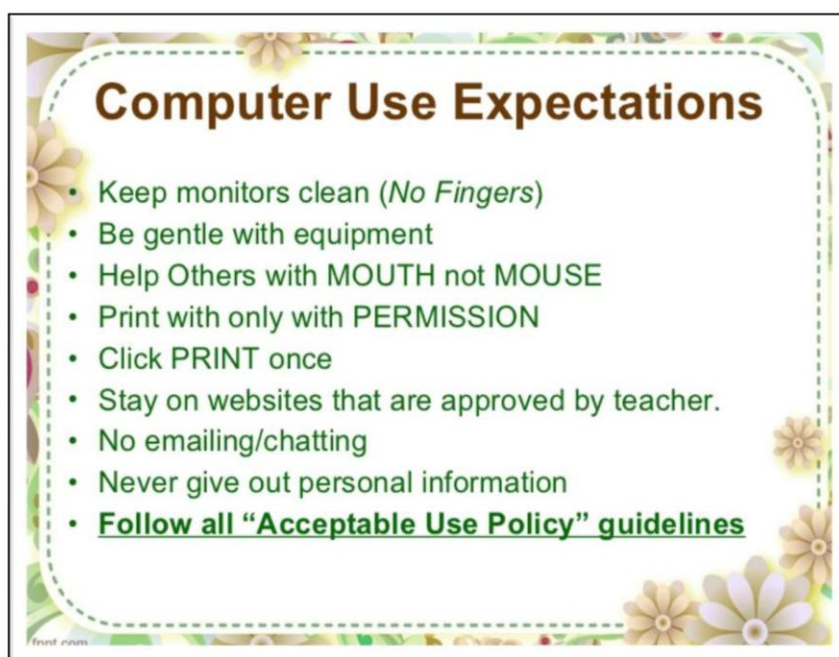
III. UTILIZAREA ALTOR ECHIPAMENTE ELECTRONICE OFERITE DE COLEGIUL ECONOMIC "MIHAIL KOGĂLNICEANU" FOCȘANI

Echipamentele electronice furnizate de Colegiul Economic "Mihail Kogălniceanu" Focșani trebuie utilizate în scopul prevăzut și menținute în stare de funcțiune pentru timpul strict necesar, în orice circumstanțe și sub supravegherea unui profesor responsabil de securitatea digitală.

Orice activitate necorespunzătoare va fi raportată directorului și adusă la cunoștință părintelui/tutorelui legal al elevului implicat.

Pentru buna desfășurare a activității didactice și creșterea eficienței actului instructiv-educativ, Colegiul Economic "Mihail Kogălniceanu" Focșani pune la dispoziția elevilor și profesorilor: laptop-uri și videoproiectoare, care sunt montate în toate sălile de clasă. Suplimentar, la cerere, sunt asigurate: boxe, casetofon, cameră web, imprimantă, scaner etc.

Cererea pentru orice material electronic trebuie făcută în timp util, completând un document adecvat, disponibil la administratorul de sistem sau administratorul școlii.



IV. ECHIPAMENTE PERSONALE

Utilizarea echipamentelor personale (laptop-uri, telefoane mobile, tablete...) de către elevii, profesorii și personalul didactic auxiliar și nedidactic de la Colegiul Economic "Mihail Kogălniceanu" Focșani, precum și de către părinții, vizitatorii sau alți membri ai Comunității Educaționale, atunci când sunt conectați la rețeaua Colegiului Economic "Mihail Kogălniceanu" Focșani, se face numai ținând cont de Politica de utilizare acceptabilă a tehnologiei informației și comunicațiilor.



Follow our 10 rules and stay safe online



1. Never give out personal information.
2. Tell a grown-up if you find something that is not right.
3. Never agree to meet people.
4. Never send your picture.
5. If someone says something mean online, tell a grown-up.
6. Don't do things online that you know are wrong.
7. Check before you download anything.
8. Don't give out your password.
9. Parents: Set up rules for going online.
10. Show your parents and carers how you use the internet. Share!



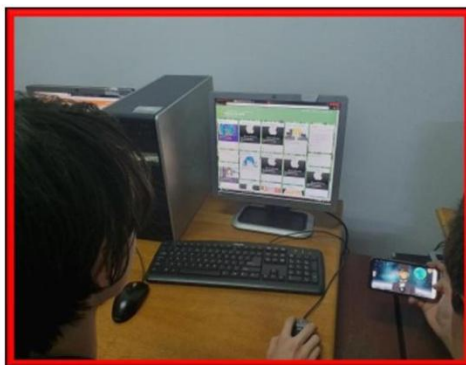
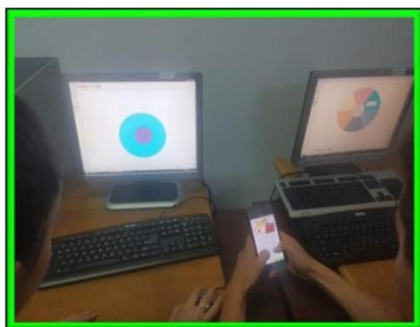
A devenit din ce în ce mai dificil și nepractic să punem în aplicare o interdicție absolută a dispozitivelor mobile în școală, deoarece acestea sunt indispensabile nu numai în viața tinerilor, dar mulți părinți insistă, de asemenea, că trebuie să poată comunica în permanență cu copiii lor.

Conform Regulamentului Școlar, elevii au voie să intre în școală cu dispozitive mobile, dar este interzisă utilizarea lor în timpul orelor. De aceea, pentru buna desfășurare a activității didactice, la începutul fiecărei ore de curs/laborator tehnologic, telefoanele trebuie închise și depozitate într-un spațiu special destinat.

În cazul confiscării unui dispozitiv mobil, elevul trebuie să oprească dispozitivul înainte de a-l înmâna profesorului, pentru a asigura protecția datelor private de pe dispozitiv. Dacă dispozitivul nu este returnat la sfârșitul zilei școlare, părinții trebuie informați și dispozitivul mobil va fi păstrat într-un loc sigur.

Profesorii pot încorpora dispozitivele mobile, în mod constructiv, în activitățile formale și non-formale.

Deși prezența telefoanelor mobile și a altor dispozitive poate fi perturbatoare și poate duce la un comportament neadecvat, cum ar fi înșelăciune și intimidare, ele pot oferi, de asemenea, oportunități fără precedent, atunci când sunt utilizate în mod proactiv și creativ în clasă, pot fi o resursă excelentă pentru a sprijini învățarea, atât timp cât este respectată o politică strictă privind posesia și utilizarea lor.



V. PUBLICAREA CONȚINUTULUI

Directorul este responsabil pentru conținutul digital publicat de Colegiul Economic "Mihail Kogălniceanu" Focșani, pe site-ul oficial al instituției, și se asigură că orice material publicat este corect și adecvat.

Nu trebuie publicate informații personale.

Paginile sau blogurile oficiale gestionate de profesori ar trebui să fie protejate în mod adecvat, împotriva utilizării necorespunzătoare, și ar trebui utilizate numai în scopuri instituționale, profesionale sau educaționale.

Utilizarea pe scară largă a Internetului și a noilor tehnologii informaționale stimulează spiritul competitiv și capacitățile profesionale și ameliorează calitatea vieții multor cetățeni.

Participarea tuturor cetățenilor la așa-numita „economie digitală” depinde de dezvoltarea sistemului educațional, care ar educa abilitatea de a analiza critic multiplele categorii de informații pe care le recepționăm (de exemplu, conținutul audiovizual), de a ne forma opinii proprii și de a ne încadra activ în soluționarea problemelor comunitare.

<https://www.cemk.ro/>



VI. ACȚIUNEA ÎN CAZ DE INCIDENTE

Toate incidentele care apar (acces accidental sau deliberat la conținuturi necorespunzătoare sau private, comunicare necorespunzătoare, viruși sau atac rău intenționat, cyberbullying...) trebuie raportate direct directorului Colegiului Economic "Mihail Kogălniceanu" Focșani, care, folosind resursele umane și materiale existente, decide și aplică măsurile necesare pentru rezolvarea lor.

Pentru evitarea incidentelor pe Internet, se vor avea în vedere:

- îmbunătățirea abilităților de navigare în labirintul informației disponibile pe Internet;
- dezvoltarea capacității de a discerne informația și de a sesiza dezinformarea;
- analiza informației din punctul de vedere al relevanței și validității;
- utilizarea corespunzătoare a informației la elaborarea proiectelor;
- înțelegerea multiplelor avantaje pe care le oferă un browser și Internetul.



VII. CYBERBULLYING

Cyberbullying-ul este termenul englezesc folosit pentru hărțuirea prin intermediul rețelilor de Internet, iar acesta a început să ia amploare tot mai mare și în spațiul românesc. Cei mai afectați sunt copiii, iar părinții și sistemul educațional încearcă în mod repetat să îi protejeze de acest fenomen.

Hărțuirea pe internet a atins deja cote alarmante, iar victimele fenomenului nu au foarte multe arme la dispoziție pentru a se proteja de așa ceva. Hărțuirea online afectează persoanele de toate vârstele, însă în cazul copiilor efectele pot fi mult mai grave. Fiind sensibili din punct de vedere psihologic, copiii și adolescenții pot recurge la gesturi dintre cele mai neașteptate, atunci când simt că activitatea de pe Internet le afectează viața.

Datele statistice din anul 2018 arată că, 80% dintre adolescenți au fost hărțuiți pe Internet. Aspectul fizic, pasiunile și situația materială se află printre principalele motive. Principalele arme de atac folosite pe Internet pentru a agresa victimele se leagă de înfățișare și felul în care se îmbracă (67%). Alte motive frecvente pentru care tinerii sunt hărțuiți sunt hobby-urile și preocupările de zi cu zi (30%), situația materială a familiei din care provin (13%), rezultatele de la școală (12%) și orientarea sexuală (8%).

Cele mai populare rețele de socializare unde are loc fenomenul de cyberbullying sunt Facebook, Messenger și, la mare distanță, Instagram, iar mijloacele de propagare a fenomenului cel mai des folosite sunt mesajele de amenințare și cele negative primite în canalul privat, urmate de comentarii negative la fotografii și furt de identitate.

Site-ul <https://oradenet.salvaticopiii.ro/viata-ta-online/prietenii/ce-este-cyberbullying-ul> oferă câteva informații privind **cyberbullying-ul** și cum trebuie acționat în caz de hărțuirea online.

Cyberbullying-ul sau hărțuirea online este bullying-ul realizat prin dispozitive mobile sau internet. Cyberbullying-ul este foarte neplăcut pentru că poate fi public, greu de dat jos de pe Internet și te poate afecta tot timpul, chiar și când ești acasă.

În plus, acesta rămâne postat mereu online și va avea repercursiuni asupra viitorului tău. Cum ai putea să eviți să treci printr-o situație de acest fel?

De ce este cyberbullying-ul atât de îngrozitor?

- O mulțime de oameni pot să vadă ce se întâmplă sau chiar să participe.
- Se poate să nu știi cine te hărțuiește pentru că acesta și-a creat un cont fals și trimite în mod anonim mesaje.
- Este greu de îndepărtat pentru că este postat pe Internet și poate fi ușor preluat sau salvat de către alte persoane.
- Este greu să scapi, dacă simți nevoia să folosești tehnologia des.
- Conținutul poate fi văzut de foarte multe persoane.
- Conținutul poate fi găsit de străini la o căutare Google.
- Informațiile postate pe Internet rămân online și nu mai ai controlul asupra lor.

Cum arată cyberbullying-ul?

- Primirea unor mesaje răutăcioase de la persoane cunoscute sau de la necunoscuți.
- Primirea unor mesaje amenințătoare sau jignitoare prin intermediul rețelelor sociale, precum Facebook sau AskFm.
- Trimiterea către alții o unor poze sau clipuri cu tine cu scopul de a te jigni sau a te face să te simți stânjenit.
- Răspândirea de zvonuri despre tine prin SMS sau aplicații de chat precum WhatsApp sau Viber.
- Furtul parolelor tale pentru a-ți prelua conturile.
- Crearea unui profil fals cu pozele tale sau postarea de statusuri și comentarii ca venind din partea ta.

Cum poate afecta cyberbullying-ul?

O persoană care este hărțuită online poate experimenta multe trăiri negative, precum:

- Sentimente de vinovăție.
- Persoana se poate simți prinsă într-o situație fără scăpare.
- Se poate simți singură, ca și cum nimeni nu o susține.
- Se poate simți exclusă.
- Sentimente de depresie, supărare și respingere de către grup.
- Sentimente de frică și nesiguranță.
- Anxietate și stres.

Ce pot face?

- Nu posta informații personale precum adresa sau numărul de telefon și nu le împărtăși pe acestea cu persoane necunoscute. Ai grijă ce tip de poze postezi sau distribui.
- Păstrează-ți parolele doar pentru tine. Nu le spune nici măcar prietenilor.
- Nu răspunde unor mesaje atunci când ești nervos sau supărat. Un răspuns din partea ta poate încuraja hărțuitorul să continue.
- Deloghează-te pentru o perioadă de timp.
- Raportează și blochează persoanele care te deranjează.

Nu este tolerat cyberbullying-ul (precum și toate celelalte forme de bullying) exercitate asupra oricărui persoane din Colegiul Economic "Mihail Kogălniceanu" Focșani. Dacă apar astfel de situații, acestea trebuie raportate directorului, care va acționa în consecință.

INTERNET SAFETY RULES
Middle School * High School

- 1 I WILL THINK BEFORE I POST.**
I agree not to post information and images that could put me at risk, embarrass me, or damage my future, such as
 - » cell & home phone numbers
 - » home address
 - » sexual messages
 - » inappropriate pictures and videos
- 2 I WILL RESPECT OTHER PEOPLE ONLINE.**
I will not
 - » post anything rude, offensive, or threatening
 - » send or forward images and information that might embarrass, hurt, or harass someone
 - » take anyone's personal information and use it to damage his or her reputation
- 3 I WILL BE CAREFUL WHEN MEETING ONLINE FRIENDS IN PERSON.**
I agree to
 - » ask my parent or guardian's permission
 - » have a parent or guardian accompany me
 - » meet in a public place
- 4 I WILL PROTECT MYSELF ONLINE.**
If someone makes me feel uncomfortable or if someone is rude or offensive, I will
 - » not respond
 - » save the evidence
 - » tell my parent, guardian, or another trusted adult
 - » report to the website, cell phone company, cybertipline.com, or the police

NetSmartz Workshop
A PROGRAM OF THE
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN
Watch videos and play games at NSTeens.org
Copyright © 2010 National Center for Missing & Exploited Children. All rights reserved.

SIGNED _____
SIGNED _____

VIII. SUPERVIZARE

Directorul Colegiului Economic "Mihail Kogălniceanu" Focșani este responsabil pentru acordurile de licență, achizițiile de software, politicile de utilizare acceptabile și accesul la rețea wireless.

Colegiul Economic "Mihail Kogălniceanu" Focșani își poate exercita dreptul de a monitoriza utilizarea sistemelor informatice în scopul verificării respectării Politicii de utilizare acceptabilă a informațiilor și tehnologiilor de comunicare, acționând în conformitate cu legea, ori de câte ori este detectat acces neautorizat și / sau utilizarea necorespunzătoare a sistemelor informatice.

De ce e necesar un Regulament / ghid de utilizare a Internetului? În ultimul deceniu tehnologia Internet, care recent a fuzionat cu tehnologia mobilă, a transformat multiplele fațete ale vieții sociale în toate țările, modificând stilurile de muncă și de viață ale oamenilor. Utilizarea acestei complexe rețele de informație și comunicare trebuie să fie făcută responsabil și trebuie să fie în atenția tuturor utilizatorilor: părinților, profesorilor și tinerilor din toată Europa.

Fișele de instruire în domeniul Internetului ale Consiliului Europei reprezintă un ghid în explorarea acestei remarcabile rețele de informare și comunicare.

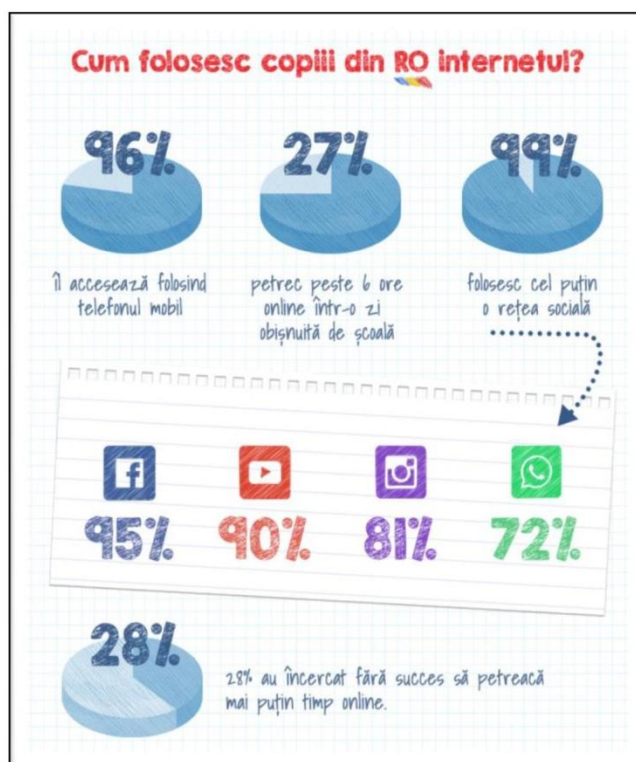
Fișele au drept obiective:

- de a oferi profesorilor și părinților un know-how tehnic suficient pentru a le permite să însoțească tinerii și copiii în călătoriile de descoperire a noului prin intermediul tehnologiilor de comunicare;
- de a evidenția problemele etice și de a sesiza în esență valoarea pedagogică a Internetului și a tehnologiei celulare;
- de a propune idei de activități practice și constructive, în sălile de clasă sau la domiciliu, pentru explorarea Internetului și a tehnologiei celulare;
- de a sugera metodele mai eficace de utilizare a Internetului, într-o gamă variată de domenii;
- de a furniza contacte (link-uri), care ar oferi informație amplă sau exemple practice.

Fișele informaționale de instruire în domeniul Internetului prezentate aici vor constitui un suport de lucru pentru profesori și elevi.

- Fișa informațională nr. 1 – Conectarea (Anexa 1)
- Fișa informațională nr. 2 – Crearea paginilor web (Anexa 2)
- Fișa informațională nr. 3 – Căutarea informației (Anexa 3)
- Fișa informațională nr. 4 - Poșta electronică (Anexa 4)
- Fișa informațională nr. 5 – Chat-urile (Anexa 5)
- Fișa informațională nr. 6 – Muzica și imaginile pe Internet (Anexa 6)
- Fișa informațională nr. 7 – Viața privată (Anexa 7)
- Fișa informațională nr. 8 – Securitatea (Anexa 8)
- Fișa informațională nr. 9 – Intimidarea și hărțuirea (Anexa 9)
- Fișa informațională nr. 10 – Tehnologia mobilă (Anexa 10)

Fișele inserate relevă considerentele etice și de securitate care trebuie respectate în utilizarea Internetului, evidențiază posibilitățile de valorificare a Internetului și a tehnologiei celulare în scopuri didactice, oferă idei pentru activități constructive în sălile de clasă și la domiciliu, sugestii practice și un spectru larg de definiții și link-uri spre paginile Web, ce conțin exemple și informație detaliată.



IX. DIVULGAREA DATELOR

Securitatea online a utilizatorilor și respectarea regulilor de utilizare a echipamentelor electronice și a Internetului reprezintă o prioritate în politica Colegiului Economic "Mihail Kogălniceanu" Focșani și este cuprinsă în Planul de Acțiune al Școlii.

Acest document va fi prezentat Comunității Educaționale prin publicarea pe pagina web a instituției și va face parte din Regulamentul de Ordine Interioară al Colegiului Economic "Mihail Kogălniceanu" Focșani.

Stimate utilizator,

Internetul a transformat radical modul de acces la informații și comunicare – creând noi oportunități pentru consolidarea democrației. Din păcate, acesta poate fi, de asemenea, folosit pentru constrângerea drepturilor omului și comiterea de infracțiuni pe Internet.

Internetul nu are frontiere și a devenit un instrument global de exercitare a drepturilor dvs. și anume:

- ❖ Access la Internet la preț accesibil și nediscriminatoriu, inclusiv pentru persoanele cu dezabilități
- ❖ Libertatea de exprimare și informare, dreptul la opinie pe Internet, în același timp cu respectarea demnității și vieții private ale altor utilizatori
- ❖ Libertatea de întrunire, asociere și de participare, votare pe rețelele de socializare și pe alte pagini web
- ❖ Dreptul la viața privată și protecția datelor cu caracter personal
- ❖ Dreptul de acces online la educație și cunoaștere
- ❖ Protecția copiilor și a tinerilor pe Internet
- ❖ Dreptul dvs. la protecție și îndrumare specială în timpul utilizării Internetului

Dacă conținutul publicat on-line compromite demnitatea, securitatea, confidențialitatea sau poate fi utilizat în viitor împotriva dvs., la solicitare, acesta trebuie șters în cel mai scurt timp posibil. Trebuie să fiți protejat de orice intervenție la bunăstarea dvs. fizică, mentală și morală, în special în ceea ce privește exploatarea sexuală și abuzul online (grooming), inclusiv împotriva mesajelor xenofobe ce incită la ură.

Pentru responsabilizarea utilizatorilor, a fost conceput **Formularul de consimțământ privind utilizarea Internetului la Colegiul Economic “Mihail Kogălniceanu” Focșani** (Anexa 11)

Toți elevii Colegiului vor lua la cunoștință prevederile prezentului Regulament și vor complepleta și semna Formularul de consimțământ privind utilizarea Internetului la Colegiul Economic “Mihail Kogălniceanu” Focșani.

Pentru elevii minori, Formularul de consimțământ privind utilizarea Internetului la Colegiul Economic “Mihail Kogălniceanu” Focșani va fi completat și semnat și de către părinți / tutori.

X. BIBLIOGRAFIE

*** Manual de legislație europeană privind protecția datelor, Agenția pentru Drepturi Fundamentale a Uniunii Europene, 2014, Consiliul Europei, 2014, ISBN 978-92-871-9938-6 (CoE), ISBN 978-92-9239-339-7 (FRA)

*** Ghid de utilizare a Internetului, Proiectul „O bună guvernare în societatea informațională”, Direcția Generală a Afacerilor Politice Consiliul Europei, 2016

<https://www.esafetylabel.eu/school-policy>

<https://www.esafetylabel.eu/mobile-devices-in-school>

<http://www.esafetylabel.eu/group/teacher/school-policy>

http://www.esafetylabel.eu/c/document_library/

<https://oradenet.salvaticopiii.ro/viata-ta-online/prietenii/ce-este-cyberbullying-ul>

<https://oradenet.salvaticopiii.ro/la-avizier/ora-de-net-lanseaza-campania-o-lume-fara-frica>

<https://rm.coe.int/16806ff6e7>

<http://eap-pcf-eu.coe.int>

http://www.cdep.ro/afaceri_europene/afeur/2018/fi_2491.pdf

<https://www.salvaticopiii.ro/ce-facem/protectie/siguranta-pe-internet>

<https://ro.wikipedia.org/wiki/Bullying>

<https://en.wikipedia.org/wiki/Cyberbullying>

XI. ANEXE

Anexa 1

11.1. Fișa informațională nr. 1 – Conectarea

Internetul este o rețea globală de computere unite prin intermediul serverelor, care funcționează ca noduri de conectare (http://en.wikipedia.org/wiki/Node_%28networking%29).

Avantajele pedagogice ale utilizării Internetului

- Internetul oferă o multitudine de idei noi și resurse pentru profesori; planuri pentru lecții, exerciții online pentru elevi și jocuri electronice educative.
- Internetul facilitează schimbul de experiență și comunicarea între profesori și elevi, făcând abstracție de frontierele dintre țări.
- Internetul oferă elevilor oportunitatea de a participa la proiecte pentru însușirea limbilor străine și cunoașterea altor culturi. Această metodă este mai rapidă și mult mai eficientă decât schimburile tradiționale de elevi și nu implică cheltuieli pentru călătorie.
- Internetul face accesibile instrumentele de cercetare chiar și pentru aceia care nu obișnuiesc să viziteze cu regularitate biblioteca tradițională.

Probleme etice și riscuri

- Ca și în societate, pe Internet există fraude, informații false și materiale inadecvate copiilor.
- Deși Internetul oferă mai multe posibilități, soluțiile tehnice nu sunt întotdeauna mai bune decât cele tradiționale. Poșta electronică, de exemplu, a revoluționat procesul de comunicare, dar nu va înlocui niciodată comunicarea față în față dintre două persoane.

Cum veți realiza conectarea?

- În cazul în care vă conectați dintr-o instituție (școlară, administrativă), probabil computerul dvs. este unit la un server "din oficiu".
- Pentru a vă conecta la Internet de la domiciliu, veți avea nevoie de:
 - ✓ un computer dotat cu modem;
 - ✓ legătură telefonică;
 - ✓ un abonament la un prestator de servicii Internet (PSI).

- Prestatorii de servicii Internet (http://en.wikipedia.org/wiki/Internet_service_provider) realizează legătura necesară dintre utilizator și Internet.
- Această funcție o pot exercita companii private, de prestare a serviciilor de telecomunicații sau operatori ai rețelelor prin cablu, sau instituții, de exemplu, școli.
- De regulă, PSI-urile solicită o taxă lunară pentru abonament și oferă o varietate de servicii.
- Utilizatorul poate accesa Internetul prin intermediul unei linii telefonice analogice (http://en.wikipedia.org/wiki/Dial-up_access). De obicei, utilizatorul este taxat conform timpului de conectare, ca în cazurile unei convorbiri telefonice obișnuite. O linie analogică nu permite conectarea simultană la Internet și telefon. Viteza conexiunilor este mică.
- O conexiune la debit înalt (http://en.wikipedia.org/wiki/Broadband_Internet_access) oferă acces prin rețeaua digitală. Ca exemple în acest sens servesc ISDN (<http://en.wikipedia.org/wiki/ISDN>) și DSL ([http://en.wikipedia.org/wiki/Digital Subscriber Line](http://en.wikipedia.org/wiki/Digital_Subscriber_Line)). De regulă, abonamentele pentru acest tip de conexiune permit acces nelimitat, pentru o taxă fixă. Totuși, PSI-urile pot stabili o limită pentru volumul de date ce poate fi accesat. Viteza de conectare este mult mai mare, aceste linii oferind posibilitatea de a telefona fără a deconecta Internetul.
- Un număr tot mai mare de computere, în special cele portabile, sunt dotate cu cartele pentru rețeaua fără fir (Wifi) (<http://en.wikipedia.org/wiki/wifi>), permițând conectarea la Internet fără cablu la domiciliu sau în locurile publice, unde nu există rețea prin cablu, cum ar fi cafenelele și aerogările.

Sugestii practice

- Alegeți o conexiune adecvată pentru utilizarea Internetului. Conexiunea la debit înalt pare a fi avantajoasă în cazurile în care Internetul este folosit cu regularitate.
- Dacă dispuneți de conexiune la debit înalt, deconectați-vă pentru perioada de timp în care nu navigați pe Internet. Conexiunea inactivă prelungită ar putea să nu vă coste suplimentar, însă sporește riscurile.
- În cazul în care computerul sau rețeaua de care sunteți responsabili sunt exploatate și de alte persoane, elaborați o politică de utilizare acceptabilă a Internetului (PUA) (<http://en.wikipedia.org/wiki/AUP>).

Informații complementare

- ❖ <http://www.thelist.com/>: pagina web The List constituie un repertoriu mondial al prestatorilor de servicii Internet.

Paginile web didactice, cum ar fi European Schoolnet <<http://www.eun.org/portal/index.htm>>, Global Schoolhouse <<http://www.globalschoolnet.org/GSH/>> și Education World <http://www.educationworld.com/>, oferă resurse și proiecte de colaborare.

- ❖ http://www.ictadvice.org.uk/index.php?section=ap&catcode=as_pl_acc_03&rid=1963&rr=1&PHPSESSID=820174b4b4df8ca7de75604c566d00ee: site-ul Becta aparține unei agenții britanice specializate în utilizarea tehnologiilor informaționale și de comunicare în domeniul educației, conține sfaturi despre elaborarea unei politici de utilizare acceptabilă a Internetului.
- ❖ <http://www.saferinternet.org/ww/en/pub/insafe/>: portalul „Insafe” propune resurse și sfaturi privind conectarea și navigarea sigură pe Internet.

11.2. Fișa informațională nr. 2 – Crearea paginilor web

Doriți să creați un site?

Tot mai frecvent administratorii, profesorii și elevii doresc să-și prezinte rezultatele activității școlare pe Internet, numărul de pagini web personale crescând incredibil. Un site bun e un mijloc minunat de realizare a relațiilor cu publicul, el poate fi utilizat pentru diferite scopuri: prezentarea de informații despre școală, comunicare sau pentru publicarea planurilor lecțiilor și cursurilor. Desigur, acesta este și un foarte bun instrument pedagogic. Deoarece paginile web pot fi folosite în multiple moduri, deseori administratorii, profesorii, elevii sau părinții nu știu cum să înceapă crearea unei pagini personale. Înainte de a proceda la crearea unei pagini web, trebuie să răspundeți la următoarele întrebări:

- Care e scopul paginii?
- De ce aveți nevoie de o pagină web?
- Cine este auditoriul dvs.: publicul din orice colț al lumii, populația regiunii, locuitorii orașului sau doar elevii și părinții?
- Care va fi conținutul paginii?

Să transformăm școlile locale în școli internaționale

- Grație Internetului, elevii de pe întreg globul pământesc pot să comunice și să colaboreze fără dificultate. Astăzi sala de clasă nu poate fi comparată cu o încăpere tradițională, delimitată de patru pereți și situată într-un punct geografic fix. Când explorăm Internetul, pereții sălilor de clasă dispar, școlile locale devenind internaționale.
- Un site școlar bun este interactiv și grație unor astfel de instrumente ca forumurile de discuție (http://en.wikipedia.org/wiki/Message_boards) permite elevilor, părinților și profesorilor, oriunde s-ar afla, să fie la curent cu cea mai recentă informație.
- Elevii pot exercita un rol activ în crearea site-urilor. De fapt, diversele concursuri, de exemplu, cele inițiate de Think Quest <<http://www.thinkquest.org/>>, CyberFair <<http://www.globalschoolnet.org/index.html>> și altele, demonstrează faptul că paginile create de elevi sunt deseori de o calitate mai bună decât paginile elaborate de profesori.
- Principiile fundamentale de creare a unei pagini web pot fi incluse în curriculum: Elevii pot crea pagini web în cadrul cursurilor de matematică, de biologie, de limba

română sau de muzică. De fapt, un număr cât mai mare de subiecte îmbogățesc paginile web.

- Este extraordinar că la crearea site-urilor elevilor nu li se cere să facă echipă doar cu colegii; ei pot conlucra cu elevi din orice colț al lumii, prin intermediul poștei electronice (<http://en.wikipedia.org/wiki/Email>), conferințelor video (http://en.wikipedia.org/wiki/Video_conferencing) și chat-urilor (<http://en.wikipedia.org/wiki/Chat>).

Probleme de securitate

La crearea oricărui gen de pagină web este important să se ia în considerare măsurile de securitate.

- Politica școlii în materie de securitate și utilizare acceptabilă a Internetului trebuie definită cu claritate până la crearea paginii web oficiale sau până la atragerea elevilor în competiții de elaborare a paginilor.
- Machetarea și maniera în care sunt prezentate imaginile trebuie să reflecte politica școlii privind securitatea.
- Pentru a asigura securitatea și respectarea vieții private, multe școli nu divulgă numele persoanelor din fotografiile pe care le publică în Internet sau indică doar prenumele lor. Este un principiu care merită să fie luat în considerare la crearea paginilor proprii. Care sunt regulile de securitate ale instituției în acest sens?
- Pentru a verifica integritatea informației publicate și a vă asigura că măsurile de securitate a paginilor la care faceți trimitere corespund cu politica adoptată de școala dvs., e necesar să verificați toate hiperlegăturile externe spre alte pagini web.
- Veți filtra accesul la Internet sau veți spune elevilor să utilizeze Internetul judicios și cu discernământ? Pentru a spori eficacitatea, multe școli combină aceste două tehnici.
- Rețineți că paginile web create de studenți în cadrul cursurilor pot fi vizualizate de utilizatori din întreaga lume. Aceste site-uri ar putea servi școlii dvs. ca instrument de relații cu publicul. De aceea, e binevenit ca profesorii să supravegheze și să ghideze elevii pe parcursul procesului de creație.
- În ultimă instanță, profesorii sunt responsabili de paginile create de elevi. De aceea, profesorii trebuie să dispună de autoritatea necesară pentru a putea respinge paginile inadecvate ale studenților și de a le retrace pe cele plasate deja pe site-ul școlii sau al proiectului. Pentru a putea supraveghea activitatea elevilor, profesorii trebuie să

cunoască parolele (<http://en.wikipedia.org/wiki/Password>) paginilor web (<http://en.wikipedia.org/wiki/Website>).

Crearea unui site școlar

Când sunt folosite corect, paginile web școlare constituie un instrument bun de expresie a diferitelor fațete ale comunității. Acestea pot cultiva sentimentul de coeziune, reprezentând un valoros instrument de comunicare și făcând informația accesibilă tuturor.

Sugestii utile privind conținutul paginilor web

- Profesorii pot prezenta planuri de lecții/cursuri sau analize ale realizărilor elevilor într-o anumită perioadă.
- Administratorii vor insera calendarul activităților sau anunțuri.
- Elevii ar putea publica lucrări artistice, articole, rapoarte despre activitatea lor etc.
- Părinții pot plasa anunțuri despre activitățile comune ale părinților și profesorilor, despre festivaluri sau alte evenimente.
- Comunitatea, în sens larg, poate transforma pagina web într-un forum, inserând anunțuri despre competiții sportive, echipele de fotbal, excursii școlare, avize emise de autorități etc.

Conținutul divers poate îmbogăți pagina web, dar prea multe persoane antrenate în elaborarea acesteia o pot face incoerentă. Este important ca de colectarea și redactarea materialelor să fie responsabilă o echipă mică. Ar fi rațional ca funcția de coordonator al aplicării tehnologiilor informaționale și de comunicare să fie atribuită unui profesor sau administrator sau unei alte persoane responsabile.

Până la lansarea paginii web urmează a fi luate în considerare următoarele:

- Software: majoritatea webmasterilor și redactorilor web preferă să lucreze cu formatul HTML WYSIWYG (<http://en.wikipedia.org/wiki/WYSIWYG>), de exemplu Dreamweaver și FrontPage. Acestea permit redactarea într-un mediu familiar fără ca utilizatorul să cunoască obligatoriu limbajul HTML.
- Deseori sunt utilizate sisteme de gestionare a conținutului paginii web, unele dintre acestea fiind elaborate special pentru instituțiile școlare.
- Hardware: e preferabil să dispuneți de scanere (http://en.wikipedia.org/wiki/Image_scanner), aparate foto digitale, camere video digitale, tripoduri și dictafoane, considerate resurse de bază.

- Hosting (http://en.wikipedia.org/wiki/Web_hosting): școlile trebuie să găsească o organizație care i-ar oferi spațiul necesar pentru a arhiva paginile web, imaginile, fișierele video etc. și a le face accesibile în Internet via pagina web. În acest sens este important a prospecta piața prestatorilor de servicii pentru a fi siguri că ceea ce oferă ei corespunde necesităților instituției școlare.

Sugestii practice

Prin investigații, școala dvs. va elabora o metodă ce-i va permite să ajungă la publicul destinat în mod eficient. Un site școlar model include:

- Informații de contact, cum ar fi adrese și numere de telefon.
- Informații despre școală, de exemplu, planuri ale lecțiilor, cursurilor etc.
- Informații despre echipa școlii: administratori, instructori etc.
- Informații despre asociațiile de părinți și profesori.
- Informații despre activități recente, desene și fotografii furnizate de elevi.
- Link-uri spre pagini educaționale similare.
- O "carte de oaspeți", în care vizitatorii să-și pună semnătura.

De asemenea, trebuie luate în calcul și criteriile tehnice:

- Un design grafic clar și plăcut.
- Accesibilitatea paginii pentru utilizatorii cu handicap.
- Fișiere grafice și alte fișiere nevoluminoase, pentru a evita încetinirea vitezei de extragere a informației.
- O machetă clară și o metodă de navigare ușor de utilizat, care ar indica clar data la care a fost actualizată pagina.
- Versiuni în diferite limbi, în caz de necesitate. Pentru ca materialul să fie accesibil elevilor din diferite țări, deseori este preferată limba engleză, ca limbă de comunicare.
- Respectarea drepturilor copiilor, a diversității sociale și culturale, a integrității fizice și personale, a valorilor democratice, ca egalitatea, libertatea și prietenia. În cazul în care instalați un forum de discuții pe site-ul școlii dvs., vă sfătuim să faceți referire la pagina Chatdanger: <<http://www.chatdanger.com/>>.

Informații complementare

Există mii de pagini web care corespund criteriilor menționate. De exemplu:

- ❖ paginile școlii primare „St. Joan of Arc” din Marea Britanie <<http://www.st-joanarc.sefton.sch.uk/index.php>> și Școlii Internaționale din Amsterdam <<http://www.isa.nl/About/abouthome.html>>.

Mai multă informație utilă în problema elaborării unei pagini web școlare puteți găsi la:

- ❖ <http://www.wigglebits.com/>: Crearea unei pagini web școlare (Building a School Website).
- ❖ <http://www.education-world.com/>: Lumea educației - cel mai bun prieten al educatorului (Education World – the Educator’s best friend).
- ❖ http://webmonkey.wired.com/webmonkey/authoring/html_basics/: pagina Webmonkey – articole, articole didactice privind limbajul HTML, design, concepție și programare.
- ❖ <http://webmonkey.wired.com/webmonkey/kids/lessons/index> html: pagina Webmonkey destinată copiilor.
- ❖ <http://www.newhorizons.org/strategies/literacy/stone> htm: Universitatea din Washington – lecții privind scrierea și redactarea textelor destinate publicării pe site.

Potențiali parteneri și o mare varietate de pagini web școlare veți găsi pe următoarele portaluri:

- ❖ <http://www.etwinning.net/ww/en/pub/etwinning/index2005> htm: pagina web Twinning Action a rețelei europene European Schoolnet.
- ❖ <http://www.ecis.org/>: Consiliul European al Școlilor Internaționale.
- ❖ <http://www.schoolswebdirectory.co.uk/>: repertoriul siteurilor școlare din Marea Britanie.
- ❖ <http://www.esp.uva.nl/>: Asociația Școlilor Europene (European Schools Project Association).

11.3. Fișa informațională nr. 3 – Căutarea informației

Introducere

Internetul este sursa unui volum de informații fără precedent, care se extinde și se schimbă continuu. Primele motoare de căutare (http://en.wikipedia.org/wiki/Search_engine) în Internet au apărut în 1993.

Majoritatea căutărilor se reduc la colectarea informației despre paginile web prin utilizarea unui robot automat (web crawler) (http://en.wikipedia.org/wiki/Web_crawler) care urmărește link-urile și adună informații despre conținut.

Multe motoare de căutare verifică nu doar paginile web, ci și forumurile de discuții (<http://en.wikipedia.org/wiki/Newsgroup>) și bazele de date. Solicitarea termenului „web site” pe Google, un motor de căutare foarte popular, <http://www.google.com>, produce peste 1 miliard de rezultate în 0.07 secunde.

Aplicații pedagogice

- Internetul este o sursă excepțională, care permite depistarea rapidă și eficientă a informației despre diferite subiecte.
- Capacitățile necesare pentru cercetarea Internetului sunt similare cu cele aplicate în bibliotecile tradiționale. Cercetarea eficace solicită o analiză cantitativă critică și instruire în domeniul Internetului.

Probleme etice și riscuri

- Păstrați o doză de scepticism față de materialele pe care le găsiți online. Internetul oferă spațiu gratuit tuturor celor care doresc să-și exprime opiniile și să lanseze idei noi. Pentru a evita propagarea miturilor și a nu deveni victima acțiunilor abuzive, evaluați critic această informație.
- Mai multe pagini web oferă eseuri integrale la diferite teme. Folosind aceste fișiere, elevii își denaturează lucrările proprii și comit un act de plagiat.
- În cazul în care folosiți materialele furnizate pe Internet, trebuie să fiți conștienți de necesitatea respectării drepturilor de autor

- Acordați, pe cât e posibil, credit autorului și indicați sursa materialului citat sau folosit. Acest fapt este important, deoarece astfel:
 - ✓ acordați creditul meritat autorului și sursei;
 - ✓ va protejați contra acuzațiilor de plagiat;
 - ✓ ajutați pe alții să judece despre credibilitatea materialului.
- Paginile web utilizează o varietate de mijloace, inclusiv plata, pentru a-și găsi un loc în clasamentul privind rezultatele motoarelor de căutare. Unele motoare de căutare, cum ar fi Google, specifică expres care rezultate sunt sponsorizate. Multe alte motoare nu consemnează acest lucru.
- Cei mai comuni termeni folosiți în motoarele de căutare sunt cei ce se referă la materialele cu conținut sexual explicit. În general, la includerea rezultatelor, motoarele de căutare cenzurează acești termeni.

Cum veți căuta informația?

- Majoritatea oamenilor caută informație în Internet folosind un motor de căutare (http://en.wikipedia.org/wiki/Search_engine).
- Un metamotor (http://en.wikipedia.org/wiki/Metasearch_engine) permite utilizarea concomitentă a câtorva motoare de căutare.
- În general, motoarele de căutare solicită utilizatorului să aplice câteva cuvinte-cheie.
- Operatorii boolean (http://en.wikipedia.org/wiki/Boolean_datatype) restrâng aria de căutare, asociind sau excluzând cuvintele-cheie. Modul de funcționare a operatorilor boolean diferă în funcție de motoarele de căutare. Ghilimelele, semnele „plus” și „minus” sunt operatorii cel mai des întâlniți.
- Unele motoare de căutare includ repertorii ce implică căutarea conform categoriilor și subcategoriilor.

Sugestii practice

- Folosiți pagini web profesionale în locul cercetării tipice. De exemplu, când căutați sensul unui cuvânt, este preferabil să folosiți un site de dicționare, ca <<http://education.yahoo.com/reference/dictionary/>>, și nu un motor de căutare.
- Variați termenii de căutare. Diferite combinații de cuvinte-cheie vor da diferite rezultate, astfel veți obține mai multe rezultate relevante.
- Marcați paginile web utile pentru a nu fi nevoiți să le căutați din nou.
- Dacă găsiți materialul necesar, tipăriți-l sau memorați-l imediat. S-ar putea să nu-l mai

găsiți sau să fie retras de pe site fără avertisment prealabil.

- Pentru a găsi informație identică, închideți în ghilimele frazele specifice introduse.
- Dacă nu reușiți să găsiți răspunsuri prin intermediul unui motor de căutare, recurgeți la un forum online.

Informații complementare

- ❖ Cele mai populare motoare de căutare sunt Google <<http://www.google.com/>>, Yahoo <<http://search.yahoo.com/>> și MSN <<http://search.msn.com/>>
- ❖ Clusty <<http://clusty.com/>> și Grokker <<http://www.grokker.com/>> sunt instrumente de căutare inovaționale, bazate pe o abordare de alternativă a prezentării informației.
- ❖ Google Zeitgeist <http://www.google.com/press/zeitgeist.html> relevă tendințele celor mai frecvente căutări pe Google.
- ❖ Wikipedia este o enciclopedie gratuită, scrisă de către utilizatorii din întreaga lume: <<http://www.wikipedia.org/>>.

Elevii vor fi ajutați să recunoască și să evite informația falsă și conținutul care nu corespunde vârstei, care ar putea intensifica neliniștea cu privire la pandemia COVID-19. Pentru a obține informații despre virus, elevii vor avea acces la numeroasele resurse digitale de la organizații de încredere precum UNICEF și Organizația Mondială a Sănătății.

11.4. Fișa informațională nr. 4 – Poșta electronică

Introducere

E-mail-ul (<http://en.wikipedia.org/wiki/Email>), forma prescurtată pentru poșta electronică, este un sistem de expediere a mesajelor de la un calculator la altul printr-o rețea, cum ar fi Internetul. Acest termen se aplică, de asemenea, pentru mesajul propriu-zis. De regulă, un e-mail este expedit în câteva secunde, iar destinatarul îl poate accesa și răspunde atunci când este disponibil. Datorită flexibilității și eficienței sale, e-mail-ul a schimbat radical felul în care lucrăm și comunicăm. Miliarde de mesaje sunt expediate zilnic prin intermediul poștei electronice.

O adresă de e-mail este compusă dintr-un nume local și un nume de domeniu, separate prin simbolul "@". Deseori, dar nu întotdeauna, numele local indică numele utilizatorului, în timp ce domeniul indică organizația unde e angajat utilizatorul, compania sau prestatorul de servicii Internet. Numele domeniului poate indica, de asemenea, tipul organizației și/sau țara de origine. Numele@ox.ac.uk, de exemplu, relevă că deținătorul e angajat sau student la Universitatea din Oxford. Un mesaj electronic este compus din „cap” și „corp”. Prima parte include informația despre expeditor, destinatar, data și ora expedierii, precum și subiectul mesajului. A doua parte include textul propriu-zis al mesajului, care poate să conțină și „semnătura”, constând din datele de contact ale expeditorului.

Un e-mail poate fi expedit și recepționat prin intermediul unui agent de mesagerie (mail user agent) (<http://en.wikipedia.org/wiki/MUA>). Agentul de mesagerie reprezintă un program, care trebuie instalat în calculator. Deși mesajele curente pot fi accesate de la distanță, programul de mesagerie este de regulă folosit din același punct.

O altă metodă pentru expedierea e-mail-urilor este mesageria online (webmail) (<http://en.wikipedia.org/wiki/Webmail>), care permite utilizatorului să recepționeze și să trimită e-mail-uri de la orice calculator conectat la Internet.

Mesajele sunt depozitate într-un loc îndepărtat, de aceea sunt accesibile, indiferent de locul unde se află utilizatorul.

Aplicații pedagogice

Tot mai des e-mail-ul este folosit ca un canal de comunicare între profesor și elev. De exemplu, profesorii pot să informeze un grup întreg despre unele modificări în program sau să distribuie și să primească materialul pentru studii la distanță.

E-mail-ul reprezintă un instrument valoros, utilizat în proiecte interculturale între clase de elevi din diferite țări. Elevii pot recurge la Internet pentru a-și perfecționa aptitudinile – a însuși o limbă străină și a face schimb de informații despre culturile de unde provin. Unii elevi liniștiți și timizi se exprimă mai bine prin intermediul e-mail-ului, decât în discuțiile față în față din sălile de clasă.

Probleme etice și riscuri

- Discuțiile sunt mai puțin formale în e-mail-uri decât într-o scrisoare tradițională.
- Exprimarea emoțiilor prin e-mail este dificilă. Această problemă poate fi soluționată prin utilizarea unor caricaturi mici numite "emoticoane" (http://en.wikipedia.org/wiki/Emoticons#Basic_examples). Totuși, e bine să recurgeți la emoticoane mai rar, pentru a nu vă distrage de la mesaj.
- O mare parte a e-mail-urilor rămân nesolicitate, transformându-se în „spam” (http://en.wikipedia.org/wiki/E-mail_spam)
- Afară de spam-ul comercial, au devenit o problemă și e-mail-urile nesolicitate trimise între prieteni și colegi. Unii utilizatori expediază concomitent mesaje unui număr mare de persoane, chiar dacă e vorba de mesaje irelevante pentru mulți din ei, sau forward mesaje (de exemplu, glume sau imagini trăsnete) celor care nu sunt interesați.
- Unele mesaje „forwarded” sunt false sau frauduloase. În această categorie se înscriu e-mail-urile făcând parte din așa-zisele „canale” de caritate. Sub pretextul că ar ajuta copii care necesită intervenții chirurgicale, în astfel de e-mail-uri se pretinde că o companie sau o organizație va plăti o anumită sumă pentru forward-area mesajului.
- E-mail-ul este cea mai banală cale de răspândire a software-ului contagios (<http://en.wikipedia.org/wiki/Malware>) cum ar fi virușii (http://en.wikipedia.org/wiki/Computer_virus) și viermii (http://en.wikipedia.org/wiki/Computer_worm).
- Este extrem de simplu să maschezi un nume pentru a induce în eroare destinatarul. E suficient să schimbi numele din parametri sau să creezi o adresă în mesageria Internet, de exemplu elvispresley@hotmail.com.

- Chiar dacă recunoașteți adresa electronică, trebuie să fiți conștienți că calculatorul de la care acesta a fost trimis poate fi un „ordinator zombi” (http://en.wikipedia.org/wiki/Computer_zombie) atacat de hackeri sau viruși.
- Prima vedere un link poate crea impresia că direcționează utilizatorul spre o pagină web, dar de fapt deschide o altă pagină. Această tehnică e folosită deseori de aceia care practică phishingul (<http://en.wikipedia.org/wiki/Phishing>) pentru a obține ilegal informații, în special bancare, în scopul escrocării utilizatorilor.

Sugestii practice

- Scrieți mesaje electronice scurte și la obiect, evitați divagațiile.
- Mesajul dvs. trebuie să fie clar și să conțină cuvinte relevante, care vor ajuta destinatarul să determine autenticitatea lui și, ulterior, să-l găsească mai ușor în cutia poștală.
- Nu expediați mesaje ample. Aplicați funcția „răspunde tuturor” (reply-to all) doar în cazurile în care mesajul e relevant tuturor și evitați să forward/transmiteți e-mail-uri celor care ar putea să nu le aprecieze.
- Evitați să verificați poșta la fiecare 10 minute. Din cauza e-mail-urilor, multă lume își întrerupe constant activitățile curente.
- Nu includeți în mesaj informație privată, în special date bancare. E-mail-urile pot fi interceptate și forwarded cu ușurință.
- În e-mail-ul dvs folosiți doar opțiunea „text brut” (plain text only). Formatul HTML poate oferi mai multe avantaje în vederea unei prezentări mai atractive, dar el de asemenea poate fi folosit pentru răspândirea codurilor contagioase.
- Fiți vigilenți atunci când primiți mesaje electronice. Nu le deschideți, dacă nu sunteți siguri de proveniența lor.
- În special fiți precauți în cazul materialelor atașate la mesaj. Dacă nu așteptați un fisier atașat sau nu aveți încredere în el din alte motive, ștergeți mesajul fără a-l deschide.

Cum veți folosi poșta electronică?

- E-mail-ul funcționează împreună cu un agent de mesagerie (MUA) (<http://en.wikipedia.org/wiki/MUA>), un program special cu care trebuie să fie dotat computerul dvs. Majoritatea computerelor conțin un MUA instalat în prealabil, cum ar fi Microsoft Outlook.

- Procedura de înregistrare a unei adrese e-mail gratuite este foarte simplă. Pagini web populare ca Yahoo! <http://mail.yahoo.com/> și Hotmail <<http://login.passport.net/ui/login.srf?lc=1033&id=2>> propun o procedură ușoară

Informații complementare

- ❖ Cei mai cunoscuți agenți de mesagerie sunt Microsoft Outlook: <<http://office.microsoft.com/en-gb/FX010857931033.aspx>> și Mozilla Thunderbird: <<http://www.mozilla.org/projects/thunderbird/>>.
- ❖ Două dintre cele mai populare pagini de mesagerie Internet sunt MSN Hotmail: <<http://login.passport.net/ui/login.srf?lc=1033&id=2>> și Gmail din Google: <https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=http%3A%2F%2Fmail.google.com%2Fmail%2F%3Fui%3Dhtml%26zy%3Dl>)
- ❖ Pagina Organizației Economice pentru Cooperare și Dezvoltare despre spam: <http://www.oecd.org/departement/0,2688,en_2649_22555297_1_1_1_1_1,00.htm>
- ❖ Articolul BBC intitulat "E timpul să schimbăm direcția și să încetăm" (Time to switch off and slowdown): <http://news.bbc.co.uk/2/hi/technology/4682123.stm>.
- ❖ Pagina web Truth or Fiction este destinată utilizatorilor Internet care doresc să verifice veridicitatea email-urilor forwarded: <<http://www.truthorfiction.com/>>.

11.5. Fișa informațională nr. 5 – Chat-urile

Ce sunt chat-urile?

Chat-ul este un termen generic pentru comunicarea interactivă într-un canal de discuții determinat. Utilizatorii pot discuta cu grupuri de persoane în săli de chat (chatrooms) (<http://en.wikipedia.org/wiki/Chatroom>) sau pot dialoga separat cu prietenii, folosind serviciile mesageriei instantanee (http://en.wikipedia.org/wiki/Instant_messaging).

Discuțiile online sunt un mijloc de comunicare non-formal, similare conversațiilor față în față, în care sunt antrenate două sau mai multe persoane. De regulă, conversațiile online constau din texte scrise, dar pot fi secondate de fotografii, imagini video sau sunet (<http://en.wikipedia.org/wiki/Streaming>) prin intermediul camerelor video și căștilor.

Această formă de comunicare instantanee diferă de comunicarea prin e-mail-uri, care nu impune prezența destinatarului în fața computerului atunci când expeditorul trimite mesajul.

Sunt oare periculoase chat-urile?

În ultimul timp s-a vehiculat mult despre riscurile la care se expun tinerii atunci când folosesc sălile de chat. Câteva cazuri criminale, mediatizate pe larg, i-au alarmat pe părinți și profesori. Ei sunt îngrijorați că, prin intermediul sălilor de chat, copiii ar putea comunica cu pedofili. Deși aceste pericole există în realitate, e important să le relativizăm. Un număr foarte mare de persoane ce discută online își prezintă identitatea reală și majoritatea discuțiilor sunt inocente.

În loc de a insufla sentimentul de frică sau de a interzice discuțiile online, adulții ar trebui să-i învețe pe tineri cum să se protejeze. Prezintăm unele reguli în acest sens:

- Copiii nu trebuie să comunice informații personale și nu trebuie să-și plaseze fotografiile în Internet.
- Ei trebuie să fie însoțiți de un adult la prima întâlnire cu un prieten virtual.
- Tinerii trebuie să semnaleze unui adult cazurile în care s-au simțit inconfortabil într-o ședință online.

Aplicații pedagogice

Profesorii deseori subestimează importanța chat-urilor pentru tineri. Chat-ul și mesageria instantanee sunt o modalitate populară de petrecere a timpului, transformând modul de comunicare dintre tineri. Desigur, această practică poate fi aplicată în scopuri educative. Prezentăm câteva idei:

- Ședințe de brainstorming și discuții în timp real asupra unor subiecte determinate.
- Jocuri de rol și simulări.
- Schimb de opinii, dezbateri și discuții în grupuri mici.
- Tutelaj și sfaturi.
- Investigații în grup.
- Crearea unei comunități online.

Cum veți proceda?

Pe web există numeroase versiuni gratuite ale programelor de chat. Le puteți găsi scriind cuvântul „chat” în oricare motor de căutare (http://en.wikipedia.org/wiki/Search_engine). Multe programe de acest fel, de exemplu Yahoo Chat <<http://chat.yahoo.com/?myHome>>, ICQ <<http://www.icq.com/>> și AOL Chat <http://site.aol.com/community/chat/allchats.html> oferă acces la un număr mare de canale de discuție în timp real. Pentru activarea chat-ului deseori e suficient ca utilizatorii să execute o simplă operație, să se înregistreze, după care se pot conecta și participa liber la discuții.

În prezent, aplicațiile pentru mesageria instantanee (http://en.wikipedia.org/wiki/Instant_message), ce permit conversațiile private cu utilizatorii selectați, sunt mai populare decât chat-urile. Vedeți <<http://www.saferinternet.org/>, www.en/pub/insafe/news/articles/0305/uk_ukcgo.htm>. Acestea pot fi găsite prin tastarea termenului “instant messaging” în oricare motor de căutare (http://en.wikipedia.org/wiki/Search_engine).

Utilizatorii activează mesageria instantanee, după care selectează o listă de persoane cu care ar dori să discute online. Mesageria instantanee este considerată mai sigură decât chat-ul, deoarece această formă de comunicare presupune atragerea unui grup restrâns de persoane.

Cum veți folosi o sală de discuții?

- Deschideți programul de chat.
- Scrieți numele utilizatorului și parola, dacă e nevoie.

- Alegeți o sală de discuții care vă convine. În general, scopurile și temele propuse pentru dezbateri sunt foarte diverse. Există săli pentru grupuri interesate de subiectele auto, de subiecte particulare, chat-uri pentru profesori etc.
- După conectare veți vedea afișate pe ecranul central conversațiile participanților.
- Scrieți mesajul dvs. și faceți click pe "enter" sau "send" pentru a-l plasa astfel, încât participanții să-l poată citi.
- Dacă doriți, puteți alege din lista participanților, ce apare în fereastră, o persoană căreia să-i adresați un mesaj în particular.
- Multe săli de discuții pot fi folosite și pentru schimbul de fișiere P2P (peertopeer) (http://en.wikipedia.org/wiki/Peer_to_peer). Sălile de chat permit, de asemenea, schimbul de fișiere mari sau prea importante pentru a fi trimise prin e-mail (<http://en.wikipedia.org/wiki/Email>).

Cum veți utiliza mesageria instantanee?

- Deschideți programul de mesagerie instantanee (http://en.wikipedia.org/wiki/Instant_message).
- Verificați lista dvs. de contacte, pentru a vedea cine este online și disponibil pentru discuție.
- Puteți adăuga contacte noi prin intrarea în adresele lor de e-mail (<http://en.wikipedia.org/wiki/Email>) și invitându-i să se alăture grupului dvs.
- Persoanele respective vor primi o invitație prin e-mail, și dacă vor fi de acord, vor fi înregistrate în lista dvs. Astfel veți avea posibilitatea să discutați în timp real ori de câte ori veți fi online.
- Faceți click pe numele utilizatorului pentru a trimite un mesaj și a deschide un dialog.
- Scrieți mesajul dvs. și faceți click pe "enter" sau "send" pentru a plasa mesajul astfel, încât să poată fi vizualizat de alți participanți la discuție.

Apropo de problemele etice

Deoarece chat-ul e bazat pe text, gesturile și comunicarea nonverbală nu pot fi transmise în timp ce tastezi, de aceea, deseori, pot apărea neînțelegeri online. Fiecare utilizator trebuie să se comporte agreabil, politicos și manierat, ca în viața de zi cu zi, și să facă un obicei din respectarea unei bune „netichete” (<http://en.wikipedia.org/wiki/Netiquette>).

Umorul și emoțiile pot fi exprimate prin intermediul emoticoanelor (<http://en.wikipedia.org/wiki/Emoticons>), combinații de simboluri utilizate grafic pentru a crea o față. În timpul discuțiilor cu străinii în Internet, fiecare trebuie să țină minte că e posibil ca unele persoane să nu fie cele care pretind a fi.

Aplicațiile de groupware (<http://en.wikipedia.org/wiki/Groupware>), care oferă posibilitatea de a discuta în școli sau sălile de clasă, sunt mai sigure și nu creează această problemă, deoarece participanții reprezintă un grup limitat de utilizatori. Vedeți <<http://www.netlingo.com/right.cfm?term=username>>.

Este foarte important să rețineți că din punct de vedere al securității este riscant să faceți schimb de fișiere. Înainte de a expedia fișiere, asigurați-vă că acestea au fost scanate pentru depistarea virusilor. De asemenea, nu uitați să scanați fiecare fișier primit înainte de a-l deschide.

Câteva reguli generale

Limbajul utilizat în timpul chat-ului este incomplet, asociativ și foarte familiar; un participant la discuțiile online trebuie să fie nu numai rapid, ci și destul de flexibil pentru a trece de la un subiect sau chiar de la o discuție la alta.

Sprijinul profesorului este foarte important, pentru a se asigura calitatea discuțiilor și participarea echilibrată a tuturor vizitatorilor sălii de chat. Cu cât elevii sunt mai tineri, cu atât e mai important ca discuțiile să fie dirijate și moderate de un profesor.

- Urmăriți activ toate discuțiile pe parcursul întregii ședințe de chat.
- Stabiliți în prealabil orarul ședințelor; toți trebuie să fie prezenți la ora fixată.
- Fiți politicoși și amabili, de parcă ați comunica față în față.
- Rețineți că un mesaj scris cu dezinvoltură poate răni interlocutorii neintenționat.
- Mesajele scurte au efect mai mare. Nu monopolizați o ședință în timp real prin plasarea unor texte ample, scrise în prealabil, pe care ceilalți sunt obligați să le citească și la care trebuie să răspundă.
- Stilul chat-ului este similar monologului interior. Încercați să citiți cu atenție mesajele altora și să le înțelegeți sensul. Aceasta vă poate ajuta să citiți printre rânduri.
- Rețineți că nu trebuie să divulgați numele dvs. de utilizator și parola.

Sugestii pentru activități în clasă

- Alegeți un subiect și solicitați elevilor să-și pună reciproc întrebări și să facă schimb de informații prin intermediul unei săli de chat.
- Alegeți un subiect de studiu, de exemplu, poezia scriitorilor englezi din secolul XIX. Adunați material suplimentar pentru a ajuta elevii să se pregătească pentru lecții. Cereți elevilor să lucreze în perechi sau grupuri mici. Această etapă de lucru ar trebui să fie organizată conform unui model. (Discuțiile online sunt foarte eficiente în grupuri mici, de 2-6 elevi).
- La finele proiectului, elevii pregătesc în grupuri prezentări similare unei ședințe de chat. Discuțiile încep cu expunerea diferitelor subiecte. Participanții la discuție rezumă ceea ce au înșușit pe durata cursului.
- Deoarece ședințele de chat modelează conversațiile din viața cotidiană, ele oferă elevilor posibilități de autoexprimare și conlucrare, fiindu-le utile la studierea limbilor străine.

Profesorul poate încuraja elevii să participe la discuții, sugerându-le să plaseze mesaje scurte. Conlucrarea poate fi intensificată prin distribuirea de roluri: un elev poate fi inventator, altul - critic. Ceilalți elevi pot urmări și evalua discuțiile.

- ENO (Environment Online) <<http://eno.joensuu.fi/tools/chat.htm>> este un proiect internațional de educație în domeniul protecției mediului. La începutul cursului, elevii găsesc subiectele de studiu pe paginile web ale proiectului. Ei colectează date științifice și empirice, fac măsurări asupra diferitelor fenomene sau execută fotografii.
- Lecțiile virtuale sunt elaborate în formă de chat-uri interactive și sincronice în timp real <<http://www.netlingo.com/right.cfm?term=real%20time%20chat>>, chestionare electronice și discuții simultane (http://en.wikipedia.org/wiki/Message_boards). Înainte de începerea și după finalizarea cursului, elevii fac schimb de idei despre activitățile lor, monitorizează exercițiile și analizează ceea ce au învățat.

Informații complementare

- ❖ <http://k6educators.about.com/mpchat.htm>: chat-ul educatorilor din școlile elementare.
- ❖ <http://teachers.net/chatrooms/>: sala de chat a profesorilor - Teachers Net Chatroom.
- ❖ <http://chat.voila.fr/>: chat-ul Voila (în franceză).

- ❖ <http://www.irrodl.org/content/v3.1/mioduser.html>: revista internațională de cercetare în domeniul învățământului deschis și la distanță (International Review of Research in Open and Distance Learning): „Dezvoltarea climatului social în discuțiile de instruire virtuală” (The Development of Social Climate in Virtual Learning Discussions).
- ❖ <http://www.ukstudentchat.com/>: săli de discuții studențești (Marea Britanie).
- ❖ <http://www.openp2p.com/lpt/a/3071>: chat-ul ca instrument social.
- ❖ <http://www.hyperdictionary.com/computing/chat>: sensul cuvântului „chat”.
- ❖ http://en.wikipedia.org/wiki/Emoticon#Basic_examples: lista principală de emoticoane.
- ❖ <http://www.newhorizons.org/strategies/literacy/oconnor> htm: site-ul pe care un magistrul în tehnologia educațională studiază impactul limbajului Internet asupra scrisului elevilor.

11.6. Fișa informațională nr. 6 – Muzica și imaginile pe Internet

Introducere

Internetul, ca o platformă multimedia, oferă un număr mare de mijloace de comunicare, ce includ fișiere audio, video și fotografii digitale. Aceste resurse au un impact impresionant, deoarece depășesc barierele lingvistice, culturale și naționale.

Problemele juridice majore sunt determinate de violarea drepturilor de autor și de conținutul ilicit.

Drepturile de autor

- În prezent funcționează mai multe legi și acorduri internaționale care protejează drepturile de autor. În 1996 peste 100 de țări au semnat tratatele Organizației Mondiale pentru Proprietate Intelectuală (OMPI) vizând conținutul digital <<http://www.wipo.int/treaties/en/>>.
- Creatorii de materiale audiovizuale beneficiază din oficiu de drepturile de autor, exceptând cazurile concrete în care ei renunță la aceste drepturi.
- Legislația din majoritatea țărilor protejează drepturi de autor pe parcursul a 50-70 de ani după moartea autorului.
- În general, există mai mulți deținători ai dreptului de autor asupra unei compoziții muzicale. Autorul, artistul care interpretează piesa, compania de înregistrare și editorul pot deține drepturi de autor sau "drepturi asociate".
- Pe lângă drepturi patrimoniale, un creator de conținut audiovizual are "drepturi morale" (http://en.wikipedia.org/wiki/Moral_rights). Drepturile morale presupun recunoașterea autorului și interzic modificarea și publicarea lucrării fără acordul autorului.
- Piese muzicale și filmele pot fi cumpărate online. Există câteva site-uri unde poate fi procurată muzică online; de exemplu, iTunes <<http://www.apple.com/itunes/>> și Napster <<http://www.napster.com/>>, însă serviciile similare care propun filme online se află la o etapă incipientă. Deoarece tot mai mulți utilizatori posedă conexiune rapidă, care permite extragerea accelerată a fișierelor voluminoase, procedura de accesare a filmelor din Internet devine obișnuită.

- Procurarea muzicii sau a filmelor online nu oferă dreptul, sau oferă drepturi limitate, de a le copia sau a le răspândi. iTunes, site-ul de muzică online al Apple, de exemplu, permite ca o secvență muzicală să fie copiată maximum în cinci computere din cadrul unei familii: <<http://www.apple.com/itunes/share/>>.
- Industria muzicală a intentat procese penale companiilor de programe P2P, precum și unor utilizatori individuali ai acestor programe. Persoanele care fac fișierele muzicale accesibile într-o rețea P2P (uploader) riscă mai mult de a fi acționate în justiție, decât cele care doar extrag fișierele.
- Creative commons <<http://creativecommons.org/>> este o organizație nonprofit, care propune o soluție de alternativă pentru drepturile de autor.

Conținutul ilicit

- Definiția termenului de conținut ilicit variază de la țară la țară.
- Deseori acest termen se aplică pentru pornografia juvenilă, violența extremă, extremismul politic sau incitarea la ură față de grupurile minoritare.
- Multe țări au o „linie telefonică de urgență”, la care pot fi semnalate cazurile privind răspândirea conținutului ilicit: <<http://www.inhope.org/en/index.html>>.
- Aplicarea măsurilor poate fi dificilă sau lentă din cauza naturii conținutului și locației serverului-gazdă.
- „Liniile de urgență” cooperează cu prestatorii de servicii Internet și cu poliția și reprezintă modalitatea cea mai eficientă pentru depistarea conținutului ilicit.
- Inhope este o rețea de „linii de urgență” naționale.

Probleme etice și riscuri

- Între anii 2001 și 2005 vânzările mondiale de discuri s-au redus cu 25%. Mulți observatori atribuie acest fenomen creșterii numărului de accesări ilegale ale muzicii online.
- Industria muzicală a răspuns prin acționarea în justiție a mai multor site-uri și utilizatori individuali.
- Folosind programele P2P (<http://en.wikipedia.org/wiki/Peer-to-peer>) expuneți computerul dvs. riscului de a fi atacat de viruși (<http://en.wikipedia.org/wiki/Viruses>) și programe de spionaj (spyware) (<http://en.wikipedia.org/wiki/Spyware>), care deseori își aleg ca țintă fișierele ce conțin piese muzicale sau imagini.

Aplicații pedagogice

- Instituțiile educaționale, în anumite cazuri, dețin autorizația de a reproduce lucrări și a le aduce la cunoștința publicului. Pentru mai multă informație, consultați legislația din România sau directiva 2001/29/EEC din 22 mai 2001.
- Lucrările trebuie să fie utilizate în scopuri strict instructive sau științifice.
- Sursa, în special numele autorului, trebuie să fie indicată, exceptând cazurile în care acest lucru este imposibil.
- Se interzice utilizarea conținutului pentru a obține beneficii economice sau comerciale directe sau indirecte.
- Înainte de a publica fotografiile elevilor în Internet, aveți nevoie de acordul în scris al părinților sau al tutorilor.
- Instituția școlară este responsabilă de conținutul publicat pe un site școlar, inclusiv cel produs de copii.

Sugestii pentru activități în clasă

- Discutați despre aspectele morale ale pirateriei audiovizuale.
- Informați elevii despre pericolul pe care-l reprezintă virușii și programele de spionaj.
- Atenționați elevii că extragerea pieselor muzicale și a filmelor protejate de dreptul de autor este pasibilă de amendă.
- Organizați dezbateri la tema conținutului ilicit și prejudiciabil. Investigațiile arată că mulți elevi accesează accidental sau intenționat materialele de acest gen și puțini dintre ei comunică despre aceasta adulților.

Sugestii practice

- Școlile și companiile trebuie să aibă o politică acceptabilă de utilizare (PAU) a Internetului și să informeze despre necesitatea respectării drepturilor de autor și combaterii materialelor cu conținut ilicit.
- Părinții trebuie să atenționeze copiii lor asupra regulilor de utilizare a Internetului.

Drepturile de autor

- Înainte de a utiliza materialul, obțineți acordul autorului.
- Menționați numele autorului sau al producătorului materialului utilizat.
- Pentru a vă edifica asupra posibilităților de folosire de către utilizatorii Internetului a materialului creat de dvs., citiți clasificările din Creative Commons:

<<http://creativecommons.org/>>.

Conținutul ilicit

- Programele de filtrare pot să vă ajute să blocați unele pagini web ilegale.
- Nici un filtru nu e perfect. De aceea, este important să discutați cu elevii regulile de folosire a Internetului.
- Încurajați-i să vorbească despre experiențele lor online.
- Semnalați, prin intermediul unei „linii de urgență”, conținutul

Informații complementare

- ❖ <http://www.wipo.int>: Organizația Mondială pentru Proprietate Intelectuală (OMPI).
- ❖ <http://www.pro-music.org/copyright/faq.htm>: pagina Promusic este o bună sursă de informare în problema pirateriei muzicale. Aceasta propune o fișă de informare pentru copii și o pagină conținând întrebări/răspunsuri pentru adulți privind modul de extragere a pieselor muzicale.
- ❖ <http://www.inhope.org>: Inhope este o rețea de „linii de urgență” create în scopul semnalării conținutul ilicit depistat în Internet.
- ❖ http://www.coe.int/T/E/human_rights/media/: pagina „mass media” a Consiliului Europei conține informații privind activitățile de protecție a drepturilor de autor.
- ❖ http://www.europa.eu.int/comm/internal_market/copyright/index_en.htm: informații ale Comisiei Europene despre dreptul la proprietatea intelectuală.
- ❖ <http://www.europa.eu.int/scadplus/leg/en/s06020.htm>: informații despre legislația Uniunii Europene în domeniul proprietății intelectuale.
- ❖ <http://www.ifpi.org>: Federația Internațională a Industriei Fonografice (FIIF) prezintă un raport juridic general în problema muzicii pe Internet.
- ❖ <http://news.bbc.co.uk/1/hi/technology/4663731.stm>: articolul BBC intitulat „Planurile Comisiei Europene privind drepturile de autor”

11.7. Fișa informațională nr. 7 – Viața privată

Cât de privat este schimbul de informații în Internet?

- Respectul vieții private (<http://en.wikipedia.org/wiki/Privacy>) se referă la gradul de control pe care o persoană îl are asupra accesului și utilizării informației personale.
- Majoritatea utilizatorilor e-mail-urilor (<http://en.wikipedia.org/wiki/Email>) și Internetului (<http://en.wikipedia.org/wiki/Internet>) contează pe faptul că informația personală nu va fi folosită fără acordul lor și că schimbul de informații este privat și securizat. Realitatea, însă, e foarte diferită.
- De fiecare dată când accesați o pagină web sau trimiteți un e-mail, dvs. comunicați informație care ar putea include adresa fizică și adresa informațională (a computerului), telefonul și numărul cardului, date despre profilul dvs. de consumator ș.a.
- Respectarea vieții private este strâns legată de securitate.

De ce trebuie să vorbim despre respectul vieții private în clasă sau la domiciliu?

- Aspectele tehnice și sociale ale respectării vieții private oferă subiecte valoroase de instruire. Acestea pot fi examinate în cadrul disciplinei despre tehnologiile informaționale, dar și în cadrul programului consacrat competențelor păstrate de-a lungul vieții.
- Fiecare elev trebuie să aibă aptitudinile necesare pentru a naviga pe Internet cu siguranță, acestea incluzând cunoștințe în materie de autoprotejare, comunicare eficientă și responsabilitate față de alții.
- Această temă se bazează pe dimensiunea civică a fiecărui program educațional. Problemele care apar cu privire la respectul vieții private online reflectă problemele sociale care actualmente predomină în majoritatea culturilor. Studiarea motivelor hackerilor (piraiilor informaționali) (<http://en.wikipedia.org/wiki/Hacker>), ale crackerilor ([http://en.wikipedia.org/wiki/Hacker#Hacker: Intruder and criminal](http://en.wikipedia.org/wiki/Hacker#Hacker:_Intruder_and_criminal)) și ale militanților pentru respectarea vieții private permit obținerea unor bogate resurse pedagogice pentru a discuta principiile și valorile democratice.

Probleme etice

- Respectul vieții private pe Internet este unul din cele mai complexe subiecte etice și juridice.
- Fiecare utilizator are dreptul la viața privată și necesită a fi protejat de intențiile malițioase.
- Noi suntem responsabili de toate deciziile pe care le adoptăm cu referire la drepturile noastre sau ale altora, cum ar fi drepturile de autor (<http://en.wikipedia.org/wiki/Copyright>) sau dreptul la proprietate intelectuală (http://en.wikipedia.org/wiki/Intellectual_property).
- Libertatea de exprimare este o valoare acceptată din punct de vedere politic.
- În viața cotidiană însă, aceasta ridică numeroase semne de întrebare, la care nu există răspunsuri simple. Ce este acceptabil și ce nu este acceptabil? Cum să aplicăm regulile fără a încălca dreptul persoanei la libertatea de exprimare?

Sugestii pentru activități în clasă

- Conturați împreună cu elevii dvs. un cadru de cunoștințe de bază privind dreptul la viața privată. Definiți conceptele, atât cele tehnice, cât și cele sociale, și identificați prejudiciile și miturile pe care ați putea să le discutați. Astfel de întrebări simple ca "Ce înseamnă respectul vieții private?" și "Este oare necesară respectarea vieții private?" ar trebui să genereze discuții aprinse.
- Căutați pe Internet pagini web ce tratează subiectul vieții private și folosiți programele traceroute (<http://en.wikipedia.org/wiki/Traceroute>) de localizare a adreselor fizice ale acestora pentru a demonstra diversele probleme geofizice ce guvernează legalitatea în Internet.
- Explorați alte probleme (culturale, politice și istorice) ce rezultă din aceste localizări. Alegeți, de exemplu, un site de reexpediere a e-mail-urilor (re-mailer) (<http://en.wikipedia.org/wiki/Remailer>) sau un serviciu proxy anonim, lansați programul de localizare, apoi căutați motivele pentru care aceste servicii sunt localizate în țările respective.
- Studiați implicațiile legilor privind dreptul la viața privată, dreptul de autor și libertatea de exprimare în diferite țări sau pentru diferite grupuri de vârstă sau culturale.
- Instruiți elevii în vederea creării unei parole sigure (<http://en.wikipedia.org/wiki/>

[Password#Factors in the security of an individual password](#)).

Sugestii practice

- Regula de aur: nu divulgați informații personale celor pe care nu-i cunoașteți și în care nu aveți încredere.
- Faceți cu regularitate copii de rezervă (back up) (http://en.wikipedia.org/wiki/Back_up) ale sistemului dvs. și adoptați o politică de securitate.
- Actualizați parametrii de securitate ai sistemului dvs. și căutați informații noi despre instrumente adiționale <http://www.epic.org/privacy/tools.html>, care ar completa modalitățile existente de securizare a informației.
- Programele antivirus (<http://en.wikipedia.org/wiki/Antivirus>) și sistemele de protecție „parafo” (firewall) (http://en.wikipedia.org/wiki/Firewall_%28_networking%29) sunt o necesitate absolută. Desigur, ați putea lua în considerare și alte instrumente, cum ar fi blocajele ferestrelor (pop-up blockers) (http://en.wikipedia.org/wiki/Pop_up#Add-on_programs_that_block_pop-up_ads) și programele de antispiionaj (anti-spyware) (<http://en.wikipedia.org/wiki/Spyware>). Nu uitați să verificați sistemele cu regularitate.
- Pentru a vă proteja calculatorul, poșta electronică și conexiunea la Internet, utilizați parole complexe ([http://en.wikipedia.org/wiki/Password#Factors in the security of an individual password](http://en.wikipedia.org/wiki/Password#Factors_in_the_security_of_an_individual_password)).
- Înainte de a comunica informații confidențiale, verificați dacă simbolul lacătului încuiat, ce garantează securitatea serverului, este vizibil pe bara de instrumente. Acest simbol relevă că tranzacția dvs. are loc într-o conexiune securizată.

Cookie-uri

- Un cookie (http://en.wikipedia.org/wiki/HTTP_cookie) reprezintă un fișier text care rămâne în computerul dvs. după ce ați vizitat un site. Acesta nu poate dăuna computerului dvs., dar va comunica informații despre comportamentul și interesele dvs. Cookie-urile transformă navigarea dvs. pe Internet într-o experiență mai personală. Astfel, când, de exemplu, v-ați înregistrat pe un site, la redeschiderea paginii, acesta poate să vă salute prin afișarea numelui dvs.
- Este necesar să determinați gradul de confidențialitate al comportamentului dvs. online. Deoarece cookie-urile pot fi utilizate pentru a afla informații de contact și profilul utilizatorului, acestea constituie un instrument de violare a dreptului la viață privată.

- Pentru a controla datele pe care sistemul dvs. le difuzează pe Internet și a șterge cookie-urile nesolicitate, puteți folosi programe de antispyonaj (antispyware) (<http://en.wikipedia.org/wiki/Spyware>).

Protejarea datelor

- Asigurați-vă că computerul dvs. și programele e-mail sunt protejate de parole (<http://en.wikipedia.org/wiki/Password>). Majoritatea computerelor „de familie” au parametrii numelor de utilizator și ai parolelor stabiliți prin default, ceea ce permite accesarea lor prin intermediul parolelor standard cum ar fi “test”. Vedeți <<http://www.netlingo.com/right.cfm?term=default>>. Nu uitați să înlocuiți acești parametri cu o parolă mai sigură și un nume de utilizator.
- E mai bine să codati (<http://en.wikipedia.org/wiki/Encryption>) informația confidențială expediată prin intermediul Internetului. Din fericire, cifrarea a devenit o normă pentru majoritatea tranzacțiilor comerciale online (<http://en.wikipedia.org/wiki/Ecommerce>), dar totuși, înainte de a transmite informații privind numărul cardului sau al conturilor bancare, trebuie să vă asigurați că pagina web este protejată.
- Diferite compartimente ale calculatorului dvs. pot fi securizate cu ajutorul parolelor. Creați parole pentru folderele ce conțin documente valoroase, de exemplu, proiecte confidențiale, studii, creații originale etc.

Informații complementare

- ❖ http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection: pagina Direcției Afacerilor Juridice a Consiliului Europei conține informații despre activitățile Consiliului Europei în domeniul protecției datelor
- ❖ <http://www.epic.org/privacy/tools.html>: EPIC (Electronic Privacy Information Center) furnizează o listă de articole și instrumente în domeniul respectării vieții private
- ❖ <http://gemal.dk/browserspy/>: utilizați programul BrowserSpy pentru a afla datele pe care computerul dvs. le pune la dispoziția celor curioși din Internet
- ❖ Sunteți preocupat de libertățile civile? Discuțiile privind respectul vieții private ar putea prelungi pentru un timp cursul în materie de cetățenie: Electronic Frontier Foundation <<http://www EFF.org/>>, Privacy. org <<http://www.privacy.org/>>, Privacy

International <[http://www. privacyinternational.org/](http://www.privacyinternational.org/)> și Privacy.net
<<http://www.privacy.net/>>

- ❖ <http://www.cyberangels.org/>: pagina web CyberAngels conține explicații și materiale didactice simple cu privire la securitatea pe Internet
- ❖ <http://www.tucows.com/>: TuCows oferă acces la peste 40 000 de programe gratuite și diferențiate. Acest site promite activarea gratuită, rapidă, locală și sigură a programelor de depistare a virusilor și spionilor informaționali (spyware)
- ❖ <http://www.zonelabs.com/store/content/home.jsp>: Zone Alarm este unul din programele renumite de protecție „parafo” (firewall). Acesta vă permite să controlați diferite programe care transmit informația prin intermediul Internetului
- ❖ <http://www.cryptoheaven.com>: CryptoHeaven este un pachet de cifrare, care oferă poștă electronică sigură, schimb de fișiere și chat cu cifruri simetrice și asimetrice
- ❖ <http://www.lavasoft.com/>: LavaSoft Ad-aware este un program de antispionaj (anti-trackware), care scanează computerul dvs. și vă protejează viața privată

11.8. Fișa informațională nr. 8 – Securitatea

Introducere

- Securitatea dvs. online poate fi comparată cu securitatea la domiciliu. Protecția este asigurată prin închiderea și zăvorârea ferestrelor și a ușilor.
- Malware (<http://en.wikipedia.org/wiki/Malware>) este un termen generic pentru programele contagioase, de exemplu, virușii (http://en.wikipedia.org/wiki/Computer_virus), care pot infecta un computer. Malware-urile pot avea mai multe efecte, cum ar fi afectarea programelor din computerul dvs., accesul neautorizat la datele dvs. sau ștergerea datelor.
- Cele mai comune forme de malware sunt virușii (http://en.wikipedia.org/wiki/Computer_virus) și viermii (http://en.wikipedia.org/wiki/Computer_worm), programe ce se autoreplică.
- În pofida numelui, nu toți virușii și alte forme de malware sunt create cu rea intenție.
- În medie, zilnic sunt identificați 10 viruși noi.
- Mulți factori relevanți pentru securitate pot fi aplicați și pentru protejarea vieții private.

Aplicații pedagogice

- Discutați cu elevii problemele de autoprotecție și responsabilitate. Deoarece mulți tineri sunt mai bine informați decât adulții, încurajați-i să împărtășească cunoștințele și propria experiență colegilor și familiilor lor.
- Mulți hackeri și creatori de viruși sunt foarte tineri. Dezbateți acest subiect în cadrul orelor.

Probleme etice și de securitate

- Insecuritatea computerului dvs. se poate răsfrânge asupra altor computere. Virușii care afectează computerul dvs. pot fi transmiși altor calculatoare.
- Oricine depozitează date personale ale clienților este responsabil de protejarea acestora.
- Pirateria (hacking) (http://en.wikipedia.org/wiki/Hack_%28technology_slang%29) sau alt acces neautorizat la informația ce vizează alte persoane constituie o violare a dreptului la viața privată.

- E important să fiți precaut, dar nu exagerați în ceea ce privește măsurile de securitate! Una din calitățile minunate ale Internetului este accesibilitatea acestuia. Restrângerea drepturilor sau filtrajul excesiv pot fi calificate drept cenzură și reduc accesul la Internet.
- Programele de spionaj (spyware) reprezintă software-uri infiltrate în computere, de obicei în scopuri comerciale. Acestea pot încerca să difuzeze informație publicitară sau să sustragă informațiile bancare. Un dialer este o formă de spyware, prin care modem-urile culeg numerele fără consimțământul utilizatorului. În general, e vorba de numere de telefon premium.
- Cookie-urile presupun depozitarea informației personale.

Sugestii practice

- Instalați programe antivirus (http://en.wikipedia.org/wiki/Anti-virus_software) și actualizați-le în permanență.
- Instalați fără întârziere corective de securitate. Unele sisteme operaționale și programe se actualizează automat sau vă informează imediat ce un corectiv este disponibil pentru preluare (activare).
- Instalați un program de protecție „parafo” (firewall) (http://en.wikipedia.org/wiki/Firewall_%28networking%29) pentru a controla traficul informațional.
- Nu lăsați calculatorul dvs. conectat la Internet, dacă nu e necesar. Abonamentele la debit înalt permit conexiuni nelimitate, dar pot compromite securitatea datelor dvs.
- Evitați să folosiți parole (http://en.wikipedia.org/wiki/Password#Factors_in_the_security_of_an_individual_password) asociate evident cu dvs. Folosiți o combinație din litere și cifre.
- Dezactivați script-urile în browserul dvs. (http://en.wikipedia.org/wiki/Web_browser). Activați script-urile doar în cazurile site-urilor în care aveți încredere.
- Nu deschideți mesajele electronice care vă par dubioase.
- Verificați credibilitatea sursei înainte de a activa un fișier în computerul dvs. Trebuie să fiți conștient că programele P2P (http://en.wikipedia.org/wiki/Peer_to_peer) au reputația de a fi distribuitoare de programe de spionaj (spyware).
- Copiați cu regularitate fișierele importante pe un suport extern, CD-romuri, Hard-discuri externe, de exemplu.
- Dacă gestionați mai mulți utilizatori sau o rețea, nu uitați că fiecare utilizator are

anumite drepturi. Restrângerea drepturilor ce nu sunt absolut necesare vă poate ajuta să evitați probleme de securitate accidentale sau intenționate.

- Administratorii de rețea trebuie să creeze o politică acceptabilă de utilizare (PAU) (<http://en.wikipedia.org/wiki/AUP>) pentru ca beneficiarii să nu pună în pericol securitatea sistemului.
- Cele mai comune ținte ale malware-ului sunt sistemul operațional Windows și browserul Internet Explorer. Luați în calcul și programele numite "surse deschise" (http://en.wikipedia.org/wiki/Open_source) sau Mozilla Firefox: <http://www.mozilla.org/>.

Informații complementare

- ❖ <http://www.microsoft.com/security/default.msp>: pagina de securitate a Microsoft.
- ❖ <http://www.apple.com/support/security>: pagina de securitate a Apple.
- ❖ <http://www.searchsecurity.com>: informații detaliate pentru profesioniștii din domeniul tehnologiilor informaționale.
- ❖ <http://www.enisa.eu.int/>: Agenția europeană pentru securitatea rețelor și a informației.
- ❖ http://www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html: directivele OCDE pentru securizarea sistemelor informaționale și a rețelor.
- ❖ <http://informationsecurity.techtargt.com/>: revista de securitate informațională.
- ❖ <http://www.2privacy.com/>: pagina web 2privacy.com poate evalua online dacă calculatorul dvs. a fost obiectul intruziunilor externe.
- ❖ Sfaturi acordate de guvernul Marii Britanii <http://www.itsafe.gov.uk/> și cel al Statelor Unite <http://www.uscert.gov/> în materie de securitate online.
- ❖ <http://www.the-dma.org/guidelines/informationsecurity.shtml>: directive privind securitatea informației în cazul comerțului online.

11.9. Fișa informațională nr. 9 – Intimidarea și hărțuirea

Care e legătura dintre Internet și intimidare sau hărțuire?

Intimidarea (<http://en.wikipedia.org/wiki/Bullying>) și hărțuirea (<http://en.wikipedia.org/wiki/Harassment>) au un impact enorm asupra felului în care omul se percepe pe sine însuși și pe semenii săi.

În general, definiția noțiunii de intimidare variază în funcție de persoană. Totuși, pentru majoritatea oamenilor intimidarea reprezintă o acțiune întreprinsă împotriva altei persoane cu scopul de a o răni, repetată în diferite forme de-a lungul unei perioade de timp. De obicei, părinții și copiii nu percep această problemă în același mod.

Intimidarea poate implica contact fizic sau verbal. Actualmente distingem intimidare virtuală via Internet, cum ar fi e-mail-uri agresive sau perverse, comentarii în sălile de chat sau în forum-uri sau, în cazurile extreme, construcția unor pagini web cu intenția de a ultragia anumiți indivizi sau grupuri de persoane.

Profesorii s-au confruntat întotdeauna cu problema intimidării și hărțuirii în sălile de clasă sau în exterior. În prezent e necesar să știm cum să reacționăm când ne confruntăm cu intimidarea pe Internet.

Cum veți reacționa la cazurile de intimidare sau hărțuire în clasă sau acasă?

- Pentru ca elevii să studieze productiv, ei au nevoie de un mediu în care să se simtă confortabil și în siguranță.
- Dacă un elev este hărțuit sau intimidat, procesul de asimilare a materiei este afectat, deoarece el nu se poate concentra, se simte amenințat și își pierde încrederea în forțele proprii. Este responsabilitatea profesorilor și a părinților de a crea condiții benefice de studiu, fie în clasă, fie pe terenul de joc, fie online.
- Elevii trebuie să fie capabili să-și asume responsabilitatea pentru acțiunile proprii, dar intimidarea le subminează încrederea și respectul față de sine.
- Elevii care se simt amenințați (online sau în viața cotidiană) au nevoie de ajutorul unui adult în care să aibă încredere. De asemenea, trebuie să reținem că persoana care intimidează are și ea nevoie de sfaturi, ca să nu se mai comporte astfel.

- Școlile ar trebui să dispună de îndrumare în acest sens. O idee bună ar fi includerea măsurilor de precauție în politica școlii cu privire la Internet.

Probleme etice și de securitate

- Intimidarea și hărțuirea în sălile de clasă pot afecta moralul tuturor elevilor, creând o atmosferă de frică și neîncredere, care nu favorizează asimilarea materiei.
- O măsură ar fi introducerea în programa școlară a managementului depășirii furiei și rezolvării conflictelor. Programele de acest gen vor permite copiilor și adolescenților să-și descopere talentele de potențiali mediatorii ai conflictelor. Astfel, se va reduce riscul degenerării unor conflicte minore în comportamente amenințătoare, atât online, cât și în viața cotidiană.
- Instituția de învățământ trebuie să adopte o politică explicită, numită politica acceptabilă de utilizare (PAU) (http://en.wikipedia.org/wiki/Acceptable_Use_Policy), pentru a monitoriza folosirea Internetului din cadrul instituției de către elevi și cadrele didactice. Acest document trebuie să releve în mod expres că limbajul vulgar și intimidarea/ hărțuirea nu vor fi tolerate. Consecințele pe care le vor suporta cei care utilizează Internetul într-o manieră inadecvată trebuie să fie expuse clar.
- Trebuie să existe o procedură tehnică care să permită monitorizarea modului de utilizare a Internetului, pentru a ști cine e online, unde și când.
- Elevii vor fi informați despre necesitatea de a stopa orice comunicare cu persoana care îi hărțuiește sau îi face să se simtă neconfortabil.
- Elevii trebuie să aducă imediat la cunoștință unui adult în care au încredere incidentul produs și, dacă e posibil, să prezinte materiale incriminatoare. Adultul urmează să aplice procedurile stipulate în PAU a instituției de învățământ.
- Această procedură trebuie să fie similară celei din viața cotidiană. Elevul hărțuit nu va mai comunica cu agresorul și va anunța despre incident o persoană adultă de încredere. Elevul nu trebuie să aibă sentimentul că e necesar să rezolve problema de unul singur.

În rezumat, remarcăm că politica școlară privind utilizarea Internetului va include metodele de intervenție pentru rezolvarea conflictelor, instruirea elevilor și a cadrelor didactice în vederea reacționării adecvate în cazurile de hărțuire online, pentru sprijinirea persoanelor intimidat sau hărțuite și, dacă e posibil, pentru corijarea agresorilor. Cu o astfel de politică, instituțiile de învățământ vor avea puține probleme generate de intimidare și hărțuire.

Sugestii pentru activități în clasă

- Jocul de rol: elevii participă la un proces simulat de rezolvare a conflictelor. Profesorul distribuie rolurile și organizează grupuri în care elevii sunt responsabili de aplanarea conflictului. Următorul pas este inversarea rolurilor, astfel încât elevii să abordeze problema dintr-o perspectivă total diferită.
- Grupuri de discuție: elevii participă la discuții, este evaluată participarea lor la soluționarea conflictelor și sunt încurajați să-și împărtășească impresiile.

Sugestii practice

Prezentăm în continuare câteva idei pentru a putea face față intimidării și hărțuirii online, mesajelor sau e-mail-urilor amenințătoare:

- Elevii trebuie să fie instruiți să nu deschidă e-mail-urile provenite din surse neidentificate.
- În cazul în care un e-mail este deschis și are conținut ofensator, ștergeți-l!
- Dacă o persoană continuă să vă expedieze e-mail-uri ofensatoare sau hărțuitoare și e posibil (prin intermediul adresei electronice) să aflați de unde acestea au fost trimise, contactați imediat prestatorul de servicii ([http://en.wikipedia.org/wiki/Internet Service Provider](http://en.wikipedia.org/wiki/Internet_Service_Provider)) pentru a-l anunța despre incident.
- Politica școlii privind utilizarea Internetului trebuie să conțină măsuri de contracarare a hărțuirii online.
- Elevii trebuie să știe că pot discuta cu profesorul sau alt adult de încredere despre cazurile de hărțuire online, precum și despre cele produse în alte circumstanțe.

Informații complementare

- ❖ <http://www.bullying.org/>: pagina Bullying.org.
- ❖ <http://www.stopbullyingnow.com/>: site-ul Stop Bullying Now!
- ❖ http://www.media-awareness.ca/english/teachers/wa_teachers/safe_pasage_teachers/risks_bullying.cfm: Să cunoaștem riscurile! Să înfruntăm intimidarea cibernetică!
- ❖ <http://www.netaalert.net.au/01569-what-is-cyber-bullying.asp?qid=10398>: Ce este intimidarea cibernetică?
- ❖ <http://www.saferinternet.org/ww/en/pub/insafe/safety.htm>: Anunțați cazurile de intimidare și conținutul prejudiciabil în rețeaua Insafe.

11.10. Fișa informațională nr. 10 – Tehnologia mobilă

Introducere

În 1983, când telefoanele mobile abia apăruseră pe piață, puțină lume le cumpăra. În 1995, în Uniunea Europeană existau cinci abonamente la 100 de cetățeni. Potrivit Eurostat (2005), în Uniunea Europeană extinsă (constând din 25 de țări), în 2003, erau 80 de telefoane mobile la 100 de locuitori. Utilizarea telefoniei mobile este un fenomen mondial, extinzându-se cel mai rapid în Africa. Funcțiile tipice ale telefoanelor mobile sunt apelurile și serviciul de mesaje scurte (SMS) (http://en.wikipedia.org/wiki/Short_message_service).

Telefoanele multifuncționale, așa-numitele "smartphones", conțin astfel de funcții ca expedierea e-mail-urilor, a imaginilor foto și video. Frontierele dintre tehnologia mobilă și cea informațională se estompează pe măsură ce tot mai multe telefoane mobile posedă navigatoare Internet și programe de e-mail și tot mai multe computere sunt fără fir.

Aplicații pedagogice

- Instruirea bazată pe tehnologia mobilă (M-learning) se axează pe telefoanele mobile, computerele de buzunar (agendele electronice) și asistenții personali (PDA).
- Un raport publicat în 2003 de SRI International relevă că 90% din profesorii care folosesc tehnologia mobilă sunt de părerea că aceasta contribuie pozitiv la asimilarea materiei de studiu de către tineri: <http://www.intel.com/education/handhelds/SRI.pdf>.
- Instruirea bazată pe tehnologia mobilă oferă posibilitatea de a personaliza metoda de predare. O școală din Statele Unite ale Americii, de exemplu, a creat o "clasă fără hârtie", utilizând noile tehnologii pentru predarea temelor și acordarea de ajutor celor care studiau engleza ca a doua limbă: <http://www.paperlessclassroom.org/>.
- Viitorul instruirii pe baza tehnologiei mobile depinde nu doar de progresul acesteia, ci și de dezvoltarea materialului didactic ce poate fi distribuit prin intermediul mijloacelor tehnice portabile.
- Coreea este considerată unul din pionierii instruirii în baza tehnologiei moderne. Din 2004, elevii au posibilitatea de a prelua textele direct din computerele de buzunar sau din alte mijloace portabile.
- Odată cu progresul tehnologiei, jocurile au devenit tot mai populare; se estimează că jocurile didactice și alte tipuri de instruire neformală vor fi adaptate acestei noi metode

de instruire.

- Computerele de buzunar sunt apreciate atât de profesorii care se deplasează, cât și de elevii și studenții care lucrează în grupuri sau pe teren.
- Conform unor investigații, utilizarea computerelor de buzunar încurajează elevii să-și asume responsabilitatea pentru munca lor, aceștia pierzând mult mai rar notițele sau exercițiile.
- Deoarece telefoanele mobile sunt atât de populare în rândurile tinerilor, profesorii pot atrage elevii la activitățile pedagogice prin folosirea SMS-urilor etc.

Probleme

- S-a constatat că elevii intră în posesia telefoanelor mobile la o vârstă din ce în ce mai fragedă, ceea ce creează motive de îngrijorare. Nu s-a demonstrat științific că expunerea prelungită la radiație, chiar și la doze minime, ar prezenta pericol pentru sănătate.
- Dacă utilizarea computerului la domiciliu în general este controlată de părinți, utilizarea telefoanelor mobile nu mai poate fi supravegheată de ei. Încurajați de această nouă libertate, copiii pot să-și pună părinții în situații financiare stânjenitoare prin procurarea "cadourilor promoționale" în timpul campaniilor media sau a accesoriilor, de exemplu, sonerii, polifonii etc.
- Telefoanele mobile pot fi folosite ca aparate de supraveghere. Echilibrul dintre securitate și libertate este o problemă controversată.
- Tehnologia Bluetooth (<http://en.wikipedia.org/wiki/Bluetooth>) generează probleme de securitate, cum ar fi pirateria și expedierea mesajelor nesolicitate.
- Moblog-urile (<http://en.wikipedia.org/wiki/Moblog>) reprezintă "blog-uri" sau jurnale intime publicate pe Internet, care sunt susținute prin intermediul telefoanelor mobile. Tinerii care plasează informații și fotografii, prin această metodă se expun riscului.
- Intimidarea prin intermediul telefoanelor mobile devine o problemă tot mai îngrijorătoare. "Happy slappers" (bătăușii veseli) sunt tineri (în special din Marea Britanie) (http://en.wikipedia.org/wiki/Happy_slapping) care folosesc telefoanele mobile pentru a înregistra atacurile, după care plasează imaginile pe Internet pentru a-și umili victimele.
- Telefoanele mobile pot să distragă atenția conducătorilor auto și să-i pună în pericol.
- Virușii (http://en.wikipedia.org/wiki/Computer_virus) și viermii (http://en.wikipedia.org/wiki/Computer_virus)

org/wiki/Computer_worm) au început să afecteze telefoanele mobile începând cu anul 2004, un exemplu în acest sens fiind viermele "Cabir".

Cum veți proceda?

- Telefoanele mobile sunt populare și relativ ieftine, de aceea sunt procurate fără dificultate.
- Dacă ați cumpărat un aparat, puteți să plătiți cartela în funcție de timpul consumat (veți fi taxat per minut) sau să perfectăți un abonament oferit de un anumit prestator de servicii mobile și să plătiți o taxă lunară pentru servicii.

Sugestii practice

- Sfătuiți tinerii să folosească limitat telefonul mobil, fără a le interzice. Celularul este deosebit de răspândit în rândurile adolescenților și, în unele cercuri, a devenit un atribut esențial pentru comunicare.
- În cazul în care nu vă folosiți de Bluetooth, dezactivați-l, pentru a evita riscurile legate de securitate.
- Ca și în cazul e-mail-urilor, acceptați doar informația primită din surse de încredere.
- Folosiți telefonul moderat. Persoanelor din preajmă ar putea să nu le placă să vă asculte conversațiile.

Informații complementare

- ❖ <http://www.e-learningcentre.co.uk/eclipse/Resources/mlearning.htm>: site-ul Learning Centre are drept obiect instruirea prin intermediul tehnologiei mobile.
- ❖ <http://www.mobile-phones-uk.org.uk/>: site britanic independent de evaluare a telefoanelor mobile.
- ❖ http://www.nestafuturelab.org/research/reviews/reviews_11_and12/11_01.htm cuprinde o analiză a tehnologiei mobile și a programelor de instruire bazate pe această tehnologie – un raport exhaustiv al Universității din Birmingham conținând studii de caz și perspectivele educației prin intermediul tehnologiei mobile.
- ❖ <http://www.m-learning.org/>: un program de cercetare și dezvoltare a instruirii prin intermediul tehnologiei mobile a tinerilor supuși riscului excluderii sociale.
- ❖ <http://www.w2forum.com/>: forumul mondial al tehnologiilor fără fir.

- ❖ http://www.childnet-int.org/downloads/CMPTAAA_A4.pdf: publicația online "Copiii și telefoanele mobile, program de acțiuni" a organizației Childnet International.
- ❖ <http://www.imcb.org.uk/>: IMCB (Independent Mobile Classification Body).
- ❖ <http://www.mdamobiledata.org/mda/>: MDA (Mobile Data Association).
- ❖ <http://europe.nokia.com/nokia/0,,76016,00.html>: pagina societății Nokia privind protejarea telefonului dvs. împotriva Bluetooth și alt malware.
- ❖ <http://www.bluetooth.com/help/security.asp>: pagină consacrată securității Bluetooth.
- ❖ <http://www.vodafone.co.uk/download/CSR%20Parent%20guide.pdf>: ghid destinat părinților, publicat de operatorul de telefonie mobilă Vodafone.

Anexa 11

**11.11. Formularul de consimțământ privind utilizarea Internetului la Colegiul Economic
"Mihail Kogălniceanu" Focșani**

Consimțământul elevilor privind acces la Internet

Subsemnatul, _____, elev în clasa _____

Declar că am citit Regulamentul privind siguranța online și utilizarea dispozitivelor electronice la Colegiul Economic "Mihail Kogălniceanu" Focșani și mă angajez să utilizez acceptabil și responsabil Internetul la școală, pentru desfășurarea activităților didactice planificate.

Data

Semnătura

Consimțământul părinților / tutorilor elevilor minori pentru acces la Internet

Subsemnatul, _____, părinte/tutore al elevului
_____ din clasa _____

Declar că am citit regulile școlii pentru utilizarea acceptabilă și responsabilă a Internetului și permit copilului meu să fie autorizat să utilizeze Internetul la școală pentru desfășurarea activităților planificate.

Data

Semnătura