

COORDONATORI ȘTIINȚIFICI

MARIUS GÖNDÖR

DANIEL TOCOIAN

CAMELIA MOLER

#Învăț acasă#Sunt în siguranță pe net



Auxiliar didactic

**pentru orele de *Consiliere și orientare* și pentru activitatea din cadrul
comisiilor pentru prevenirea și eliminarea violenței, a faptelor de corupție și discriminării în mediul școlar și promovarea
interculturalității**

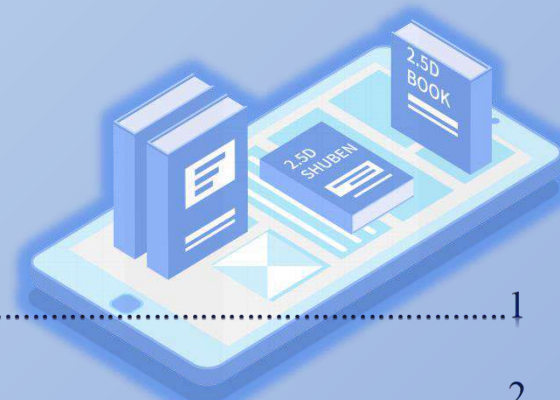
**Editura Școala Vremii Arad
Iunie, 2020**

ISBN 978-606-9067-25-3

Autori

- ❑ Camelia Moler, inspector școlar penru educație permanentă și activități extrașcolare, Inspectoratul Școlar Județean Arad
- ❑ Cătălin Tiriteu, inspector principal, Direcția Generală de Asistență Socială și Protecția Copilului Arad
- ❑ Cătălina Surcel, director executiv Asociația Telefonul Copilului
- ❑ Ciprian Tocan, agent șef, Inspectoratul de Poliție Județean Arad
- ❑ Mihaela Cadariu, profesor logoped, Centrul Județean de Resurse și Asistență Educațională Arad
- ❑ Radu Crahmaliuc, GDPR Analyst & Business Advisor
- ❑ Radu Preda, vicepreședintele Consiliului Județean al Elevilor Arad
- ❑ Sorin Hoară, Federația Națională a Asociațiilor de Părinți
- ❑ cpt.Valentin Bosoncea, ofițer specialist, Inspectoratul Județean de Jandarmi Arad

Cuprins



PREZENTAREA COLABORATORILOR.....	1
IMAGINEA CAMPANIEI.....	2
I. STATISTICI ȘI REGLEMENTĂRI LEGALE PRIVIND UTILIZAREA INTERNETULUI.....	3
I.1. Date statistice înregistrate în România.....	3
I.2. Analiza rezultatelor chestionarului adresat elevilor și diagnosticarea nevoii de informare, preveniere și consiliere	5
I.3. Riscuri și reglementări legale.....	9
II. CUM AR TREBUI SĂ FOLOSESC CORECT ȘI RESPONSABIL INTERNETUL?.....	10
II.1. Sfaturi pentru elevi.....	11
II.2. Sfaturi pentru profesori.....	14
II.3. Sfaturi pentru părinții elevilor care participă la sistemul de educație online	13
III. LA CE PERICOLE MĂ EXPUN DACĂ NU FOLOSESC CORECT ȘI RESPONSABIL INTERNETUL?.....	22
III.1. Cyberbulling.....	22
III.2. Grooming.....	24
III.3. Sexting.....	26
III.4. Sextortion.....	28
III.5. La ce alte pericole mă expun dacă nu folosesc corect și responsabil internetul?.....	30
IV. CARE SUNT PAȘII PE CARE TREBUIE SĂ-I URMĂM ÎN CAZ DE PERICOLE PENTRU A FI ÎN SIGURANȚĂ PE NET, DAR ȘI ÎN VIAȚA REALĂ?.....	33

*Comisia pentru prevenirea și combaterea violenței în mediul școlar a
Inspectoratului Școlar Județean Arad*

Campanie pentru informare și prevenire a pericolelor, privind utilizarea internetului

#Învăț acasă#Sunt în siguranță pe net

în colaborare cu:

- Inspectoratul de Poliție Județean Arad - Compartimentul de Analiză și Prevenire a Criminalității
 - Inspectoratul de Jandarmi Județean Arad
 - Centrul Județean de Resurse și Asistență Educațională Arad
- Direcția Generală de Asistență Socială și Protecția Copilului Arad-Serviciul prevenire marginalizare socială
 - Primăria Municipiului Arad
 - Consiliul Județean al Elevilor Arad
 - Federația Națională a Asociațiilor de Părinți
 - Asociația Telefonul Copilului
- Radu Crahmaliuc PhD. MSc., GDPR Analyst & Business Advisor

#Învăț acasă
#Sunt în siguranță pe net



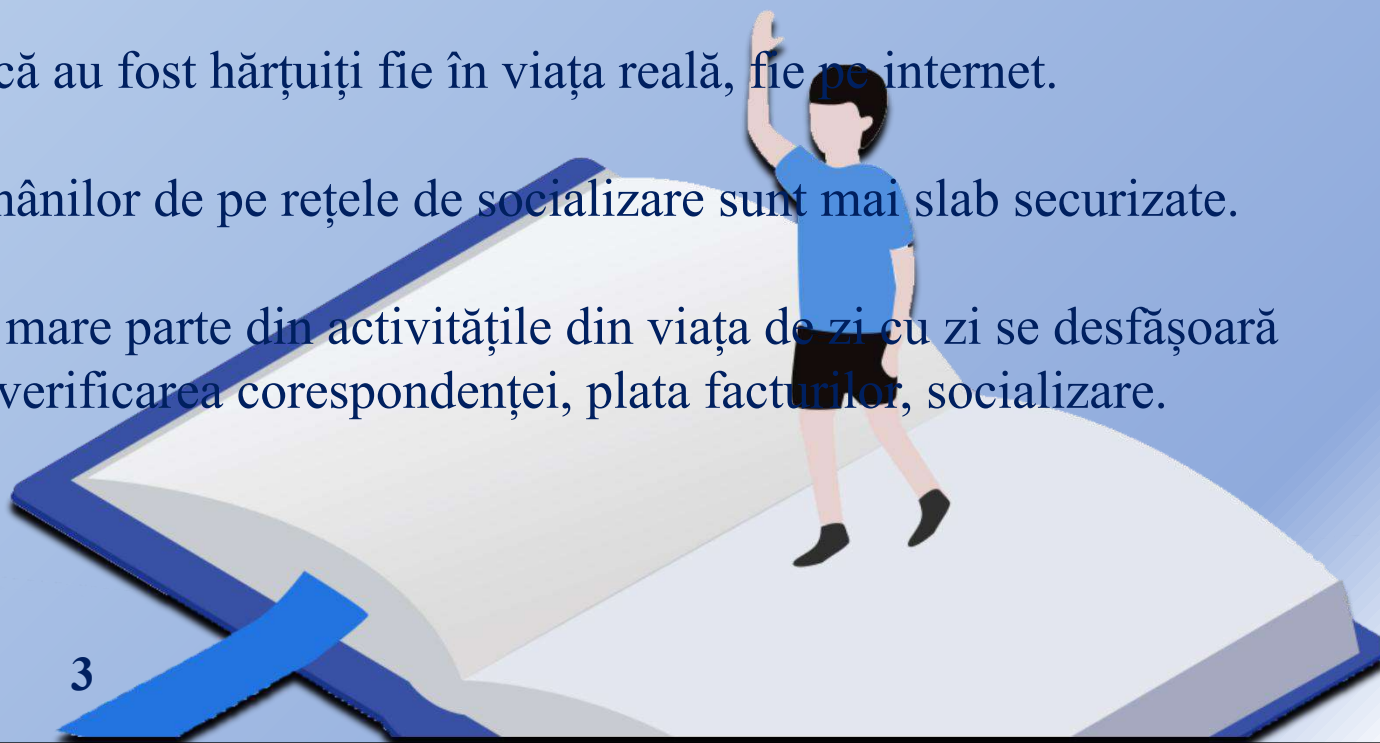
I. STATISTICI ȘI REGLEMENTĂRI LEGALE PRIVIND UTILIZAREA INTERNETULUI

I.1. Date statistice înregistrate în România

Conform studiului EU Kids Online realizat la inițiativa Uniunii Europene:

- ☐ În România se înregistrează cea mai mare incidență a hărțuirilor din Europa.
- ☐ 41% dintre copiii români intervievați declară că au fost hărțuiți fie în viața reală, fie pe internet.
- ☐ În același timp, s-a constatat că profilurile românilor de pe rețele de socializare sunt mai slab securizate.

Românii petrec în medie 5 ore zilnic online și o mare parte din activitățile din viața de zi cu zi se desfășoară aici: cumpărături online, accesarea știrilor, verificarea corespondenței, plata facturilor, socializare.

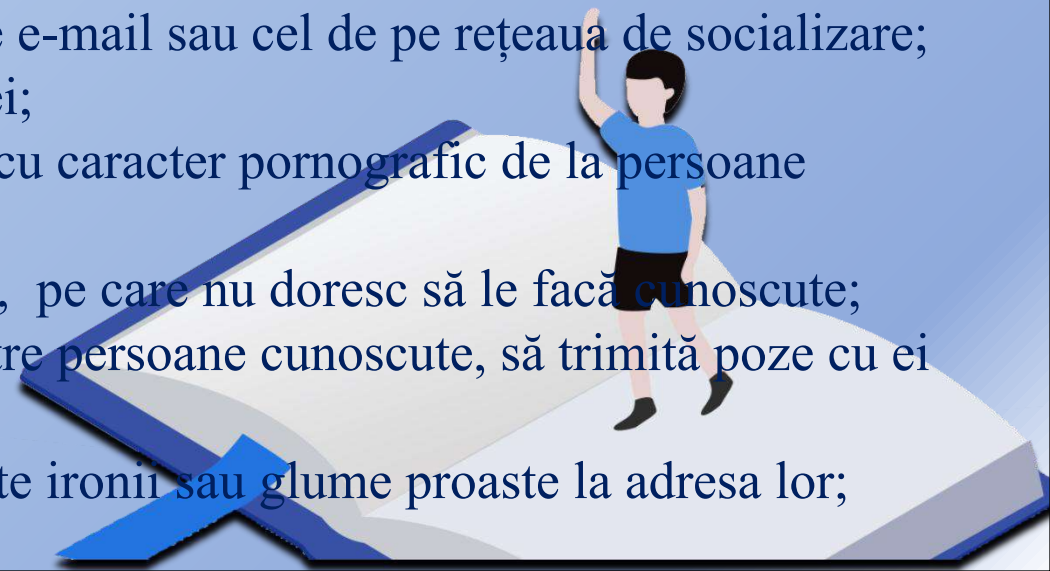


I. STATISTICI ȘI REGLEMENTĂRI LEGALE PRIVIND UTILIZAREA INTERNETULUI

Conform studiului IGPR privind siguranța on-line a copiilor

- ☐ O parte a elevilor chestionați au menționat că au fost victime ale agresiunilor online, unii dintre ei fiind chiar victime ale unor fapte grave, incriminate de Codul Penal.

- ☐ **În ultimele 12 luni:**
 - 20,9% au declarat că au primit mesaje amenințătoare;
 - 15,4% spun că au fost postate pe internet fotografii cu ei, fără acordul lor, cu scop ofensator;
 - 13,7% dintre respondenți au declarat că le-a fost spart contul de e-mail sau cel de pe rețeaua de socializare;
 - 11,5% susțin că au fost răspândite zvonuri neadevărate despre ei;
 - 11,3% au primit, printr-o formă de comunicare online, imagini cu caracter pornografic de la persoane necunoscute;
 - 10% au fost amenințați că vor fi postate pe net lucruri despre ei, pe care nu doresc să le facă cunoscute;
 - 7,9% dintre elevi au fost solicitați, doar în mediul online, de către persoane cunoscute, să trimită poze cu ei nud;
 - 7% declară că cineva a creat o pagină web, de unde să fie lansate ironii sau glume proaste la adresa lor;



I. STATISTICI ȘI REGLEMENTĂRI LEGALE PRIVIND UTILIZAREA INTERNETULUI

I.2. Analiza rezultatelor chestionarului adresat elevilor și diagnosticarea nevoii de informare, prevenire și consiliere

Conform studiului I.Ș.J.Arad privind siguranța elevilor în mediul virtual, s-au înregistrat următoarele:

☐ Aproximativ 4000 elevi respondenți, dintre care:

- 52, 8% au vârsta cuprinsă între 15-19 ani;
- 38,4 % au vârsta cuprinsă între 11-15 ani;
- 49,6 % provin din mediul urban, iar 50,4% din mediul rural;
- 44,4% sunt băieți, iar 55,6% fete.

- ### ☐ 44, 2% dintre respondenți declară că au nevoie de îndrumare din partea cadrelor specializate în ce privește siguranța în spațiul virtual, restul elevilor considerând că este nevoie de acest lucru, însă nu neapărat din surse oficiale, părinții putând reprezenta îndrumătorii copiilor utilizatori de internet.

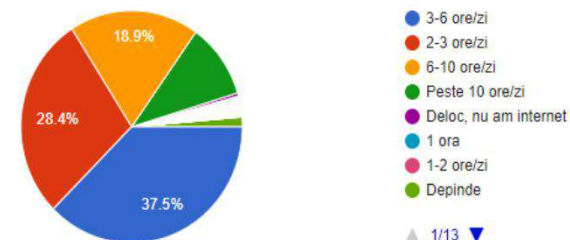


I. STATISTICI ȘI REGLEMENTĂRI LEGALE PRIVIND UTILIZAREA INTERNETULUI

- ❑ Din cei aprox. 4000 elevi respondenți, mai mult de jumătate se informează din mediul online, fie de pe site-uri de știri, blog-uri, website-uri de streaming sau site-uri pe care le găsesc utilizând diverse motoare de căutare; 924 dintre elevi se informează de la profesori.
- ❑ Aprox. 50% dintre elevi cunosc care sunt riscurile utilizării internetului, iar în ce privește posibilitatea de a se apăra împotriva pericolelor utilizării acestuia, 72,8% *declară că se feresc de interacțiuni cu surse care nu prezintă încredere. Doar 24% declară că apelează la organele de poliție.*
- ❑ Timpul petrecut pe internet în perioada actuală (11 martie - 29 mai 2020):
 - 37,5% - 3-6 ore/zi;
 - 28,4% - 2-3 ore/zi;
 - 18,9% - 6-10 ore/zi;
 - 10,4% - peste 10 ore/zi;
- ❑ Starea de spirit în perioada de învățare la distanță:
 - 30,4% - se simt singuri, deși comunică online cu colegii și profesorii;
 - 30% - se simt extrem de obosiți din cauza utilizării în exces a internetului;
 - 28,2% - sunt tot mai iritați pentru că nu comunică față în față cu prietenii;
 - 21,7% - simt o stare de disconfort psihic, pe care nu o pot descrie.

8. Cât timp petreceți pe internet în contextul actual de COVID-19 (în cadrul activităților online organizate de școală și în afara acestora)?

3,771 responses



▲ 1/13 ▼



I. STATISTICI ȘI REGLEMENTĂRI LEGALE PRIVIND UTILIZAREA INTERNETULUI

☐ Alte răspunsuri extrase la întrebarea referitoare la starea generală în perioada de învățare la distanță:

- *„Am o stare de ură pentru propria-mi persoana” (mediul rural, masculin, 11-14 ani)*
- „Mă simt foarte bine stând acasă. Vorbesc cu prietenii mei când vreau. Și în timpul liber pictez sau desenez. Uneori mă joc pe PC.”
- „Mă simt cât de cât bine! Dar aș vrea să începă școala!”
- „Mi-e dor de colegi și de profesori!”
- *„Sunt într-un impas pe care organismul meu l-a perceput ca pe un mic șoc psihic. Fiecare zi - un nou început și un alt pas mic spre bine.” (mediul urban, feminin, 15-19 ani, petrece peste 6-10 ore /zi online)*
- „Mă simt mai obosită din cauza timpului petrecut în fața calculatorului, dar am noroc că stau la casă și pot să mai fac câte o pauză în curte, pentru revigorare.”
- *„Sunt mai tristă, nu sunt obisnuită cu învățatul online și vreau să-mi vad colegii și prietenii. (mediul urban, feminin, 11-14 ani, petrece peste 10 ore/zi online)*
- *„Mă simt obosită și fără puteri, fără vlagă și îmi este greu să mă apuc să fac lecții. Nu am motivatie stând în casă” (mediul urban, feminin, 15-19 ani, petrece 6-10 ore/zi online)*
- *„Nu e legat de ore, e un sentiment depresiv legat de izolare/distanțare”(mediul urban, masculin, 15-19 ani, petrece 6-10 ore/zi online)*
- „În mare parte bine, nu mai am parte de stres. Dar, în același timp, aș dori să pot comunica cu prietenii mei față în față.”

I. STATISTICI ȘI REGLEMENTĂRI LEGALE PRIVIND UTILIZAREA INTERNETULUI

☐ **Atunci când simt că problemele îi apasă, în această perioadă de distanțare socială, comunicarea se realizează:**

- 82,2% cu părinții sau cineva din familie
- 30% cu colegii și prietenii
- 6% cu profesorii, dirigintele
- 3,6% cu nimeni, pentru că nu au cu cine



The image shows a digital survey form titled "KEEP YOUR KIDS SAFE Online". The title is in large, bold letters, with "SAFE" in green and "Online" in a smaller green font. Below the title, it says "Section 1 of 3". The main heading of the survey is "#Învăț acasă#Sunt în siguranță pe net - Chestionar adresat elevilor". The text explains that the survey is conducted by the County Commission for the prevention and reduction of violence in the school environment, in collaboration with the County School Inspectorate, the County Police, the General Directorate of Social Assistance and Child Protection, and the County Center for Resources and Educational Assistance. It aims to identify opinions on internet safety during the COVID-19 pandemic. The survey is anonymous and the responses will be used for statistical purposes. The survey is dated March 11, 2020.

I. STATISTICI ȘI REGLEMENTĂRI LEGALE PRIVIND UTILIZAREA INTERNETULUI

I.3. Riscuri și reglementări legale

Riscuri asociate navigării pe internet

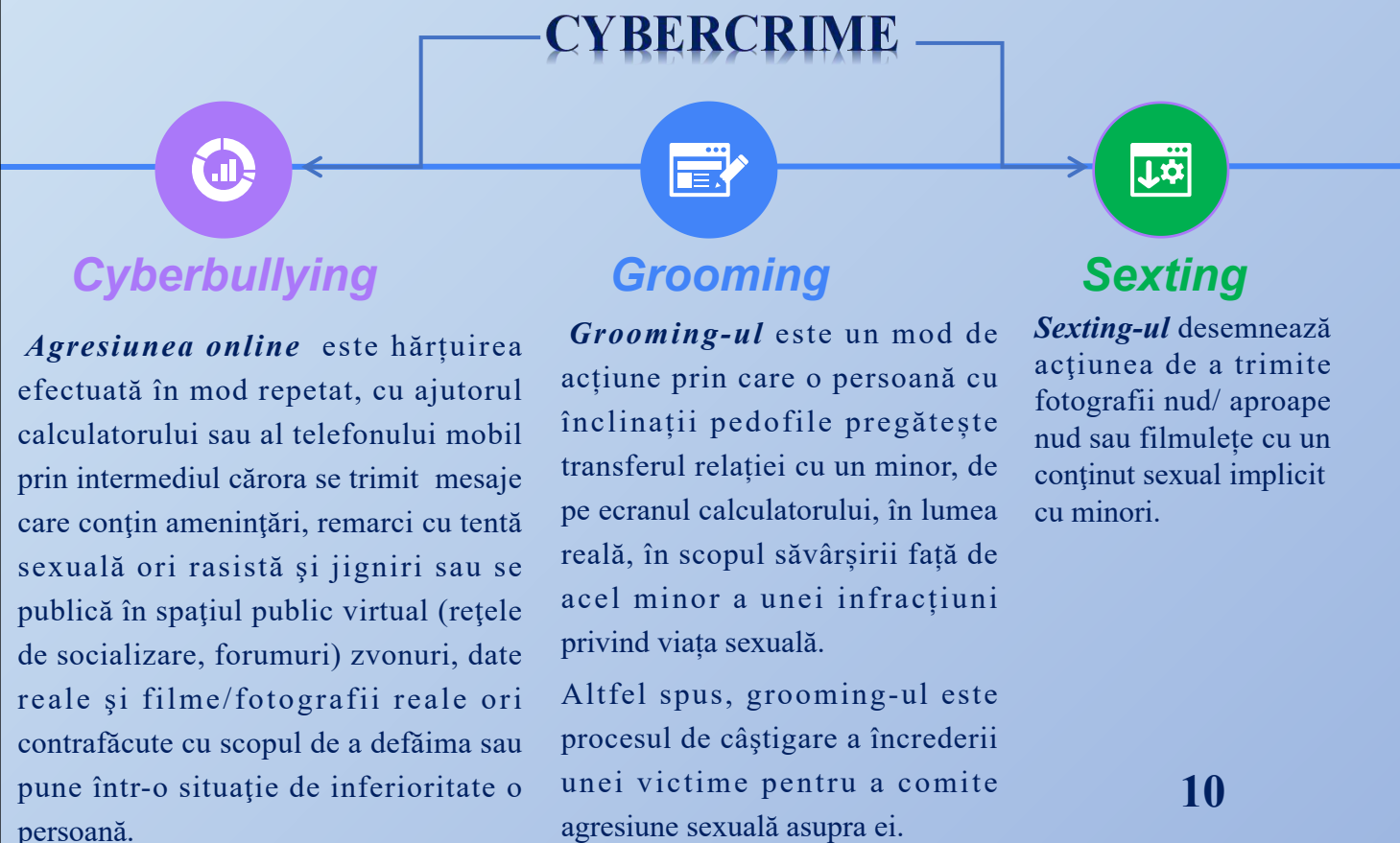
- ☐ Utilizarea de informații eronate
- ☐ Infectarea sistemului cu programe de tip malware
- ☐ Încălcarea drepturilor de autor
- ☐ Hărțuire, abuz, șantaj online
- ☐ Pornografie infantilă
- ☐ Trafic de persoane
- ☐ Fraude
- ☐ Furt de identitate
- ☐ Dependență



Infracțiuni asociate abuzurilor în mediul online :

- ☐ Amenințarea - art. 206 Cod Penal
- ☐ Șantajul - art. 207 Cod Penal
- ☐ Hărțuirea - art. 208, alin 2 Cod Penal
- ☐ Coruperea sexuală a minorilor -art. 221 Cod Penal
- ☐ Racolarea minorilor în scopuri sexuale - art. 222 Cod Penal
- ☐ Hărțuirea sexuală - art. 223 Cod Penal
- ☐ Pornografie infantilă - art. 374 Cod Penal

CUM AR TREBUI SĂ FOLOSESC CORECT ȘI RESPONSABIL INTERNETUL? & LA CE PERICOLE MĂ EXPUN DACĂ **NU** FOLOSESC CORECT ȘI RESPONSABIL INTERNETUL?

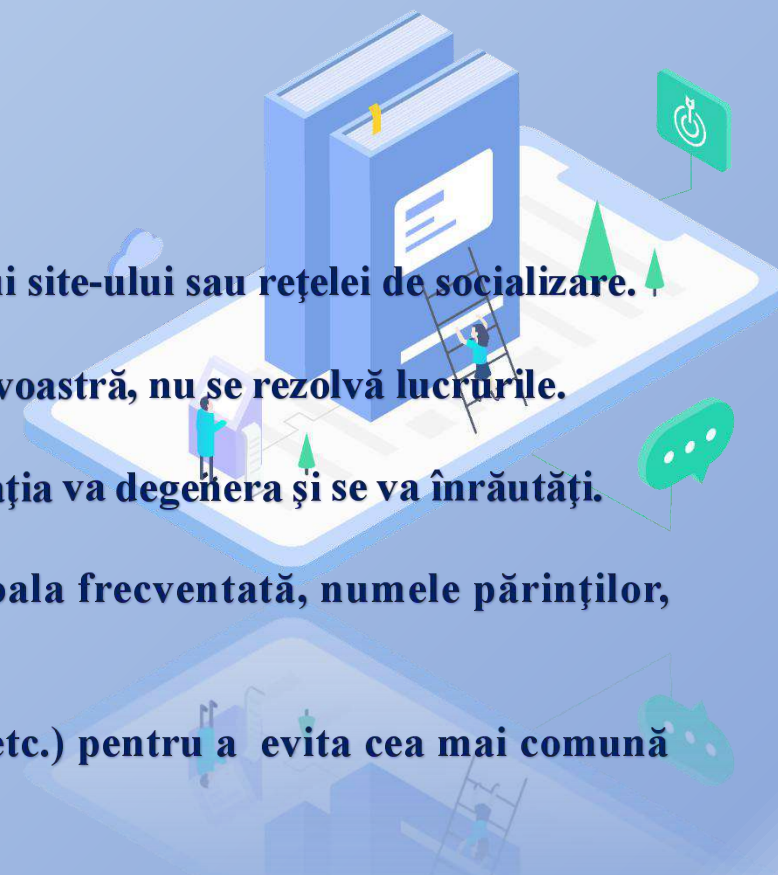


II. CUM AR TREBUI SĂ FOLOSESC CORECT ȘI RESPONSABIL INTERNETUL?

II.1. SFATURI PENTRU ELEVI

...pentru prevenirea cyberbullying-ului

- ☐ Blocați-i pe cei care vă incomodează, iar dacă este posibil, raportați-i administratorului site-ului sau rețelei de socializare.
- ☐ Discutați problemele voastre cu persoane de încredere! Păstrând totul pentru dumneavoastră, nu se rezolvă lucrurile.
- ☐ Nu vă „răzbunați” replicând în același mod cu cel care vă incomodează, deoarece situația va degenera și se va înrăutăți.
- ☐ Evitați distribuirea online a datelor cu caracter personal (adresa de domiciliu, școala frecventată, numele părinților, profesia părinților etc.)!
- ☐ Protejați-vă datele sensibile (fotografii personale, coduri de acces, numere telefon etc.) pentru a evita cea mai comună fraudă cibernetică (mesajele de tip phishing și spam)!
- ☐ Vorbiți cu prietenii voștri și cereți-le permisiunea, înainte de a posta fotografii în care apar și ei. Totodată, prietenii voștri ar trebui să vă ceară permisiunea înainte de a posta fotografii cu dumneavoastră!

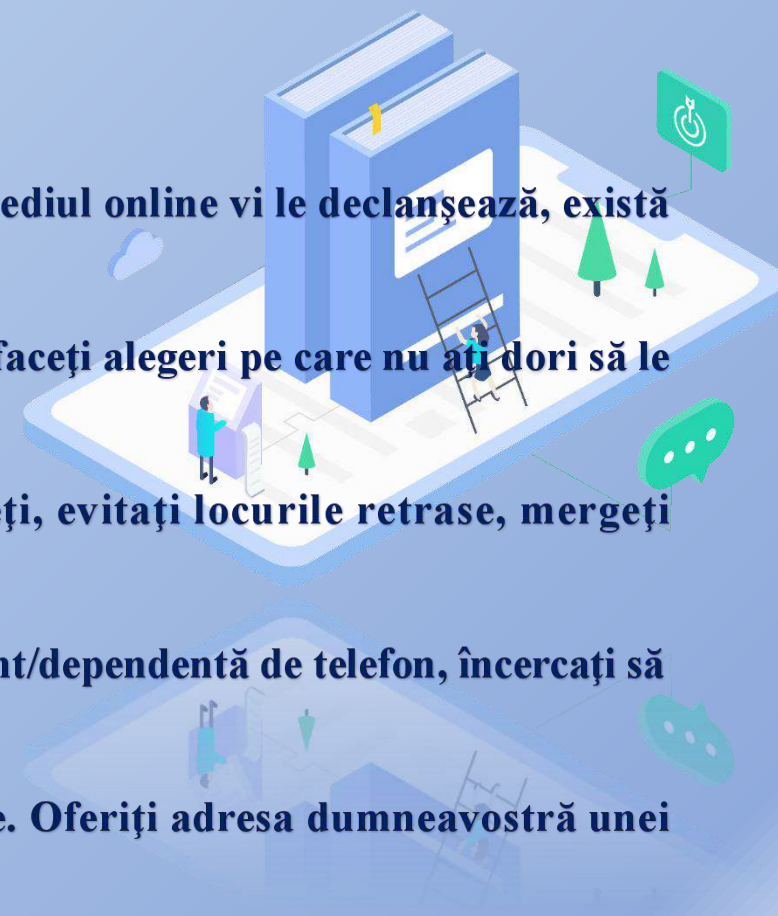


II. CUM AR TREBUI SĂ FOLOSESC CORECT ȘI RESPONSABIL INTERNETUL?

II.1. SFATURI PENTRU ELEVI

...pentru prevenirea grooming-ului

- ☐ Nu aveți încredere necondiționată în sentimentele pe care o persoană cunoscută în mediul online vi le declanșează, există riscul să rămâneți dezamăgit.
- ☐ Dacă o situație creată pe internet vă pune într-un context neplăcut sau presupune să faceți alegeri pe care nu ați dori să le faceți, discutați cu persoanele apropiate în care aveți încredere.
- ☐ Dacă un amic/amică din mediul virtual vă propune o întâlnire și doriți să mergeți, evitați locurile retrase, mergeți însoțit/însoțită și anunțați o persoană cunoscută cu privire la locul în care mergeți.
- ☐ Dacă suspectați că un prieten/prietenă se comportă ciudat, se izolează și este dependent/dependentă de telefon, încercați să discutați cu el/ea și să aflați ce i se întâmplă.
- ☐ Acționați cu prudență când navigați pe internet, la fel cum procedați și în societate. Oferiți adresa dumneavoastră unei persoane pe care o întâlniți pe stradă?
- ☐ Evitați să divulgați în mediul online datele dumneavoastră personale sau pe cele ale prietenilor, prin date personale înțelegând nu doar numele sau adresa, ci și locurile pe care le frecvențați sau fotografiile dumneavoastră.



II. CUM AR TREBUI SĂ FOLOSESC CORECT ȘI RESPONSABIL INTERNETUL?

II.1. SFATURI PENTRU ELEVI

...pentru prevenirea sexting-ului

- ☐ Evitați să postați imagini personale și intime și amintiți-vă că puteți fi înregistrat sau fotografiat cu ușurință dacă se folosește webcam în mod abuziv. O îmbrățișare inocentă poate fi folosită în foarte multe modalități.
- ☐ Relațiile sentimentale nu justifică sexting-ul, iar dacă totuși decideți „să o faceți”, vă asumați riscul de a fi „expuși” *dacă și atunci când* relația se destramă.
- ☐ În cazul în care o persoană cu care comunică pe internet te jignește, te amenință, îți transmite mesaje cu tentă sexuală, îți cere să îi trimiți poze nud cu tine sau îți trimite poze cu conținut pornografic, te îndeamnă să consumi alcool ori droguri, anunță-ți părinții sau fă o sesizare pe unul din site-urile specializate!



II. CUM AR TREBUI SĂ FOLOSESC CORECT ȘI RESPONSABIL INTERNETUL?

II.2. SFATURI PENTRU PROFESORI

- ☐ Indiferent de platforma de comunicare online folosită, școala este obligată să asigure o instruire adecvată a profesorilor/educatorilor care inițiază sesiunile de educație de la distanță.
- ☐ Nu utilizați aplicații nerecomandate. Sunteți obligați să folosiți doar aplicațiile aprobate de echipa tehnică și DPO.
- ☐ Ca profesor care conduce o lecție *la distanță* aveți rolul de Operator de date personale. Dvs.stabiliți conținutul, participarea și modul de derulare a lecției. De aici și toate responsabilitățile GDPR ce revin unui operator.
- ☐ Aveți datoria să gestionați cu responsabilitate listele cu numele și adresele de e-mail ale elevilor.
- ☐ Nu uitați ca la programarea unei sesiuni de educație să setați funcțiile de securitate ale platformei utilizate: ID conferință, parolă de acces, blocare acces nedorit etc.
- ☐ Trimiteți pe un canal sigur de comunicare invitația de participare care conține link-ul de conectare, ID sesiune și parolă.
- ☐ Conectați-vă la sesiunea online cu câteva minute înainte. Nu permiteți conectarea elevilor înaintea dvs. Dacă aplicația permite, elevii pot aștepta câteva minute într-un Waiting Room.
- ☐ La începerea sesiunii, verificați identitatea utilizatorului, iar în cazul unui participant necunoscut respingeți participarea acestuia.



II. CUM AR TREBUI SĂ FOLOSESC CORECT ȘI RESPONSABIL INTERNETUL?

II.2. SFATURI PENTRU PROFESORI

- ☐ În cazul nedorit în care un intrus a penetrat sistemul de conectare și interferează video și sonor peste conținutul lecției, blocați imediat toate microfoanele și camerele video și opriți sesiunea. Orice astfel de incident trebuie semnalat conducerii, echipei IT și responsabilului cu protecția datelor.
- ☐ Se recomandă ca lista cu numele elevilor participanți asociată la imaginile de conectare să conțină doar prenumele. În funcție de aplicația utilizată, lista poate fi reținută sau nu de platformă.
- ☐ În calitate de administrator de sesiune, puteți activa/ dezactiva imaginile celor conectați. Pentru un grup relativ restrâns de participanți, cum este cazul elevilor dintr-o clasă, pot fi lăsate camerele video active.
- ☐ În cazul în care înregistrați ora de clasă pentru a fi disponibilă online, se recomandă să dezactivați imaginile video. Nu permiteți înregistrarea sesiunii de educație de către participanți. Comunicați-le elevilor că doar dvs. puteți controla înregistrarea, care va fi ulterior partajată cu toți cei interesați.
- ☐ La terminarea lecției, nu închideți sesiunea până nu v-ați asigurat că toți elevii participanți de la distanță se deconectează de la platforma de comunicare.

Radu Crahmaliuc, consultant GDPR Ready, „Sfaturi pentru profesorii care susțin cursuri online”, gdprreadyinitiative.com, 26 martie 2020

II. CUM AR TREBUI SĂ FOLOSESC CORECT ȘI RESPONSABIL INTERNETUL?

II.3. SFATURI PENTRU PĂRINȚII ELEVILOR CARE PARTICIPĂ LA SISTEMELE DE EDUCAȚIE ONLINE

Adoptarea metodelor de educație online vine cu o serie de facilități, dar și cu provocări legate de nevoia de adaptare la un alt stil de învățare și cu alte instrumente. Fiți implicați și ajutați școala și elevii să parcurgă împreună transformarea către o lume tot mai digitală și mai conectată.

Iată un set de recomandări și sfaturi de bună practică grupate pe tematici care ne interesează pe toți în organizarea unui proces de învățare de acasă cât mai accesibil, mai eficient și mai sigur:

☐ Rutina zilnică

- ✓ Creați copiilor un program zilnic, pentru a fi mai eficienți în activitatea de învățare.
- ✓ Amenajați un spațiu confortabil, unde pot lucra liniștiți.
- ✓ Stabiliți ore regulate pentru pregătirea lecțiilor, mese, joacă, recreere și odihnă.
- ✓ Ajutați-i să ia o pauză atunci când stau prea mult la masa de lucru.
- ✓ Respectați-le programul de instruire. Nu îi distrageți pe durata sesiunilor online.
- ✓ Supravegheați-le ținuta și conduita pe durata orelor.



II. CUM AR TREBUI SĂ FOLOSESC CORECT ȘI RESPONSABIL INTERNETUL?

II.3. SFATURI PENTRU PĂRINȚII ELEVILOR CARE PARTICIPĂ LA SISTEMELE DE EDUCAȚIE ONLINE

❑ *Provocările sistemului de învățare online*

- ✓ Gândiți-vă la un sistem de monitorizare a activităților de învățare online, fără să fiți prea intruzivi.
- ✓ Stabiliți un set de reguli pentru folosirea Internetului și a rețelelor sociale.
- ✓ Supravegheați discret activitatea pe Internet a copiilor când au nevoie de documentare sau vizualizarea unor materiale cu conținut didactic.
- ✓ Explicați-le copiilor care sunt pericolele accesării unor site-uri nerecomandate.
- ✓ Învățați-i să nu răspundă la solicitări venite din partea unor necunoscuți.
- ✓ Verificați și supravegheați conturile online deschise de copii sau în numele copiilor.
- ✓ Asigurați-vă că echipamentul folosit pentru lecțiile online are toate aplicațiile actualizate și instalate legal.
- ✓ Dacă copilul folosește calculatorul dvs., securizați-vă zona personală de lucru. Creați o partiție pe discul hard și un desktop dedicat pentru copil.
- ✓ Folosiți o conexiune sigură de Internet și conectare Wi-Fi parolată.
- ✓ Monitorizați modul în care copiii folosesc canalele de comunicare: telefon, e-mail, mesagerie și alte aplicații online.



II. CUM AR TREBUI SĂ FOLOSESC CORECT ȘI RESPONSABIL INTERNETUL?

II.3. SFATURI PENTRU PĂRINȚII ELEVILOR CARE PARTICIPĂ LA SISTEMELE DE EDUCAȚIE ONLINE

❑ *Asistență și supraveghere*

- ✓ Discutați cu copiii despre cele învățate în timpul zilei și planul pentru zilele următoare.
- ✓ Asistați copiii în relațiile de socializare cu colegii. Le lipsesc recreațiile și comunicarea de după ore.
- ✓ Ajutați-i să își dezvolte abilitățile de concentrare.
- ✓ Supravegheați durata activităților petrecute online și în fața unui ecran.
- ✓ Nu vă implicați prea mult în rezolvarea temelor pentru acasă. Copiii trebuie să simtă încrederea acordată și responsabilitatea muncii lor.
- ✓ Încurajați activitatea fizică regulată.

❑ *Comunicarea cu Școala*

- ✓ Comunicați cu profesorii prin canalele folosite în mod frecvent și aprobate de școală.
- ✓ Răspundeți în timp util solicitărilor din partea școlii, primite direct sau prin copii.
- ✓ Evitați canalele de comunicare nesigure, precum sistemele de mesagerie instant.
- ✓ Solicitați sprijin de la coordonatorii școlari sau profesori atunci când apar diferite probleme.



II. CUM AR TREBUI SĂ FOLOSESC CORECT ȘI RESPONSABIL INTERNETUL?

II.3. SFATURI PENTRU PĂRINȚII ELEVILOR CARE PARTICIPĂ LA SISTEMELE DE EDUCAȚIE ONLINE

❑ *Măsuri de securitate și protecția datelor personale*

- ✓Lecțiile online și documentația aferentă sunt proprietatea școlilor.
- ✓Respectați regulile de protecție a drepturilor de proprietate intelectuală.
- ✓Nu înstrăinați sau nu permiteți accesul persoanelor neautorizate la materialele online!
- ✓Respectați regulile de folosire a Internetului și a aplicațiilor dedicate!
- ✓Nu postați pe Facebook sau Instagram imagini cu ecranul de pe durata orelor de clasă dacă pe ecran apar și imagini cu alți copii!
- ✓Asigurați accesul protejat al copiilor la Internet!
- ✓Asigurați-vă că școala depune toate eforturile pentru protecția datelor personale și că are o politică de confidențialitate publicată pe site!



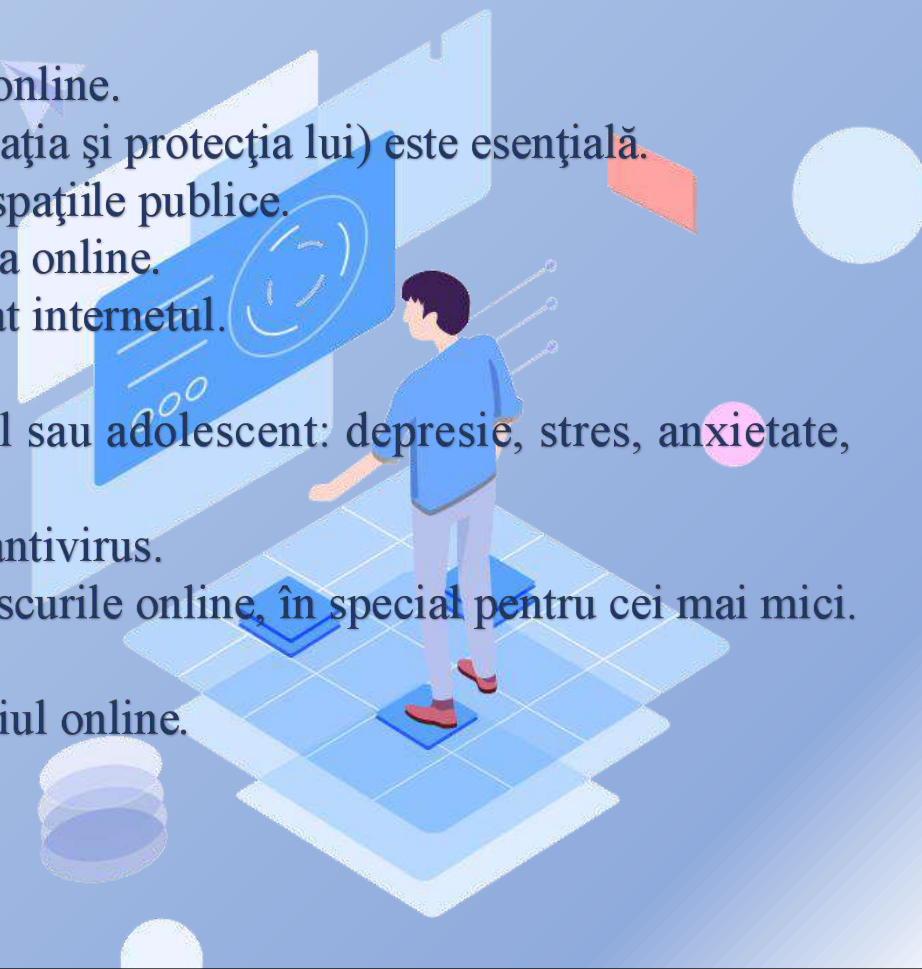
(Radu Crahmaliuc, GDPR Analyst & Business Advisor)

II. CUM AR TREBUI SĂ FOLOSESC CORECT ȘI RESPONSABIL INTERNETUL?

II.3. SFATURI PENTRU PĂRINȚII ELEVILOR CARE PARTICIPĂ LA SISTEMELE DE EDUCAȚIE ONLINE

➤ *Câteva sugestii:*

- ☐ Adulții din viața copiilor pot reprezenta modele de interacțiune în mediul online.
- ☐ Relația de încredere dintre copil și părinți (sau adulții responsabili de educația și protecția lui) este esențială.
- ☐ Educația pentru mediul online are aceleași reguli și principii ca aceea din spațiile publice.
- ☐ Purtați discuții deschise cu copiii pentru a afla cum și cu cine pot comunica online.
- ☐ Stabiliți împreună cu copiii reguli despre cum, când și unde poate fi utilizat internetul.
- ☐ Identificați instrumentele online adecvate pentru a vă recrea împreună.
- ☐ Identificați și rezolvați la timp problemele care-l fac vulnerabil pe copil sau adolescent: depresie, stres, anxietate, probleme cu alcool/droguri.
- ☐ Asigurați-vă că dispozitivele copiilor au softurile actualizate și programe antivirus.
- ☐ Configurați controale parentale pe dispozitivele copiilor pentru a atenua riscurile online, în special pentru cei mai mici.
- ☐ Arătați copilului cum să folosească setările de siguranță.
- ☐ Informați și stimulați copiii să ceară respectarea propriilor drepturi în mediul online.



II. CUM AR TREBUI SĂ FOLOSESC CORECT ȘI RESPONSABIL INTERNETUL?

II.3. SFATURI PENTRU PĂRINȚII ELEVILOR CARE PARTICIPĂ LA SISTEMELE DE EDUCAȚIE ONLINE

➤ *Explicați copiilor că...:*

- ☐ ...persoanele străine nu au de ce să figureze în lista noastră de prieteni.
- ☐ ...locația în care este ar fi sigur să rămână secretă.
- ☐ ...tot ceea ce postează în online, rămâne mereu în online.
- ☐ ...parolele puternice sunt greu de spart, dar nu imposibil.
- ☐ ...internetul este un spațiu public.
- ☐ ...pe internet nu putem verifica identitatea cuiva.
- ☐ ...pe internet se expun la riscuri (ex. Stricarea reputației cu consecințe pe termen lung, revenge-porn).

➤ Învățați copiii cum să reacționeze în situațiile în care sunt abordați de străini.

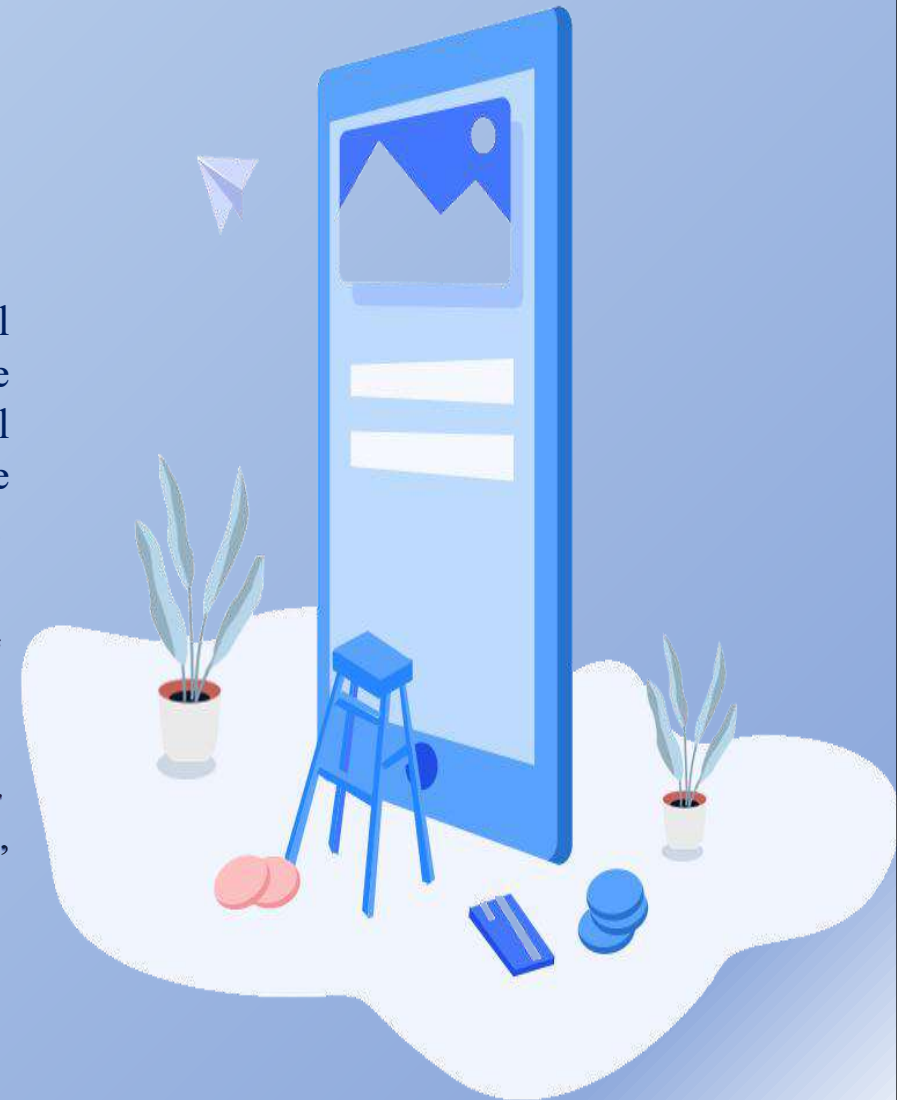


III. LA CE PERICOLE MĂ EXPUN DACĂ **NU** FOLOSESC CORECT ȘI RESPONSABIL INTERNETUL?

III.1. CYBERBULLYING

Ce este cyberbullying-ul?

- ❑ **Cyberbullying sau agresiunea online** este hărțuirea efectuată în mod repetat, cu ajutorul calculatorului sau al telefonului mobil, prin intermediul cărora se trimit mesaje care conțin amenințări, remarci cu tentă sexuală ori rasistă și jigniri sau se publică în spațiul public virtual (rețele de socializare, forumuri) zvonuri, date reale și filme/fotografii reale ori contrafăcute cu scopul de a defăima sau pune într-o situație de inferioritate o persoană.
- ❑ Hărțuirea online este o formă tot mai actuală și mai frecventă de abuz îndreptat împotriva copiilor.
- ❑ De multe ori agresorul subestimează efectele, considerând acțiunile lui o simplă distracție. Informațiile postate online rămân, existența lor fiind permanentă, dificil de eliminat, uneori imposibil.



III. LA CE PERICOLE MĂ EXPUN DACĂ **NU** FOLOSESC CORECT ȘI RESPONSABIL INTERNETUL?

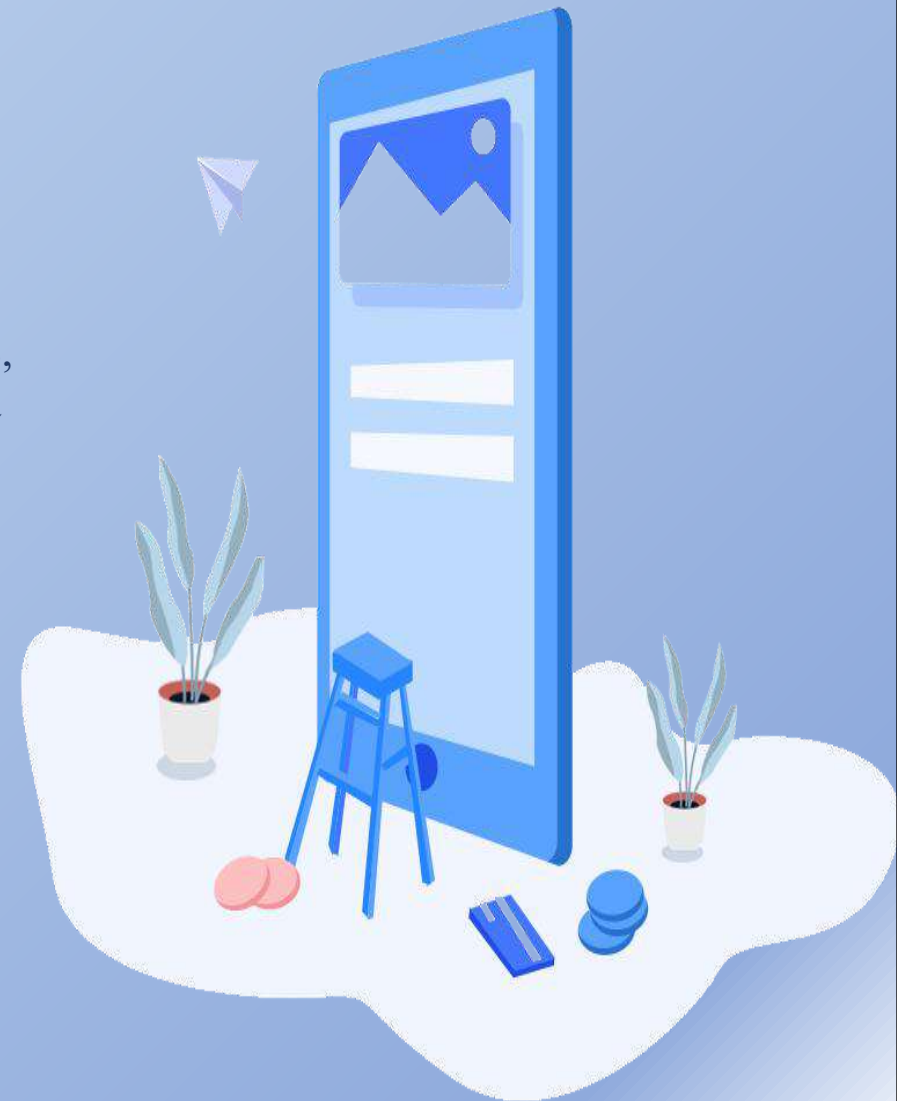
III.1.CYBERBULLYING

Unde are loc cyberbullying-ul?

Hărțuirea de acest tip are loc pe bloguri, pagini personale, forumuri, e-mail, SMS, MMS, agresiunea având uneori loc prin încărcarea unor poze sau imagini video pe Internet, fără a ține cont de dreptul la viața privată a victimei.

Cum ar arăta un exemplu de cyberbullying?

- ☐ Primirea online, prin intermediul rețelelor sociale sau pe telefonul mobil a unor zvonuri, minciuni, mesaje răutăcioase, amenințătoare sau/și jignitoare de la persoane cunoscute sau de la necunoscuți;
- ☐ Comentarii răutăcioase la propriile postări sau la postări care te privesc;
- ☐ Trimiterea spre alte persoane a unor poze compromițătoare sau clipuri cu tine, fără a avea permisiunea ta, cu scopul de a te jigni sau a te face să te simți stânjenit.



III. LA CE PERICOLE MĂ EXPUN DACĂ **NU** FOLOSESC CORECT ȘI RESPONSABIL INTERNETUL?

III.2. GROOMING

Ce este grooming-ul?

- ❑ Grooming-ul este un mod de acțiune prin care o persoană cu înclinații pedofile pregătește transferul relației cu un minor, de pe ecranul calculatorului, în lumea reală, în scopul săvârșirii față de acel minor a unei infracțiuni privind viața sexuală.
- ❑ Altfel spus, grooming-ul este procesul de câștigare a încrederii unei victime pentru a comite agresiune sexuală asupra ei.

Unde are loc grooming-ul?

Mijloacele online cele mai folosite de către agresori sunt chat-urile, videochat-urile, rețelele de socializare și webmail-ul.

Cum ar arăta un exemplu de grooming?

- ❑ Cazul unui adult de cetățenie română care, creându-și un profil de adolescentă, a intrat în contact cu un adolescent din SUA.



III. LA CE PERICOLE MĂ EXPUN DACĂ **NU** FOLOSESC CORECT ȘI RESPONSABIL INTERNETUL?

Exemplu fictiv de grooming:

„Andreiuta noastră, în vârstă de 13 ani, își creează un cont de Facebook, își încarcă niște poze nu tocmai decente din telefonul personal, iar într-o zi, observă că are o cerere de prietenie de la Ionuț, un băiat în vârstă de 15 ani, înalt, brunet cu ochii albaștri, pe care, bineînțeles că o acceptă. După binecunoscuta ploaie de like-uri din partea amândurora, Ionuț, mai curajos din fire, îi scrie mesaj pe chat fetei, vorbesc timp de câteva zile, iar acesta își face curaj pentru a o invita în parc, la o înghețată. Bineînțeles, Andreiuta este foarte fericită și acceptă invitația, se aranjează, se parfumează, iar când ajunge în parc ghiciți cu cine se întâlnește...cu nea Ion, 40 de ani, chel, cu burtă și cel mai grav, cu probleme psihice, iar de aici nu mai are rost să continui sumbrul scenariu.”



III. LA CE PERICOLE MĂ EXPUN DACĂ **NU** FOLOSESC CORECT ȘI RESPONSABIL INTERNETUL?

III.3. SEXTING

Ce este sexting-ul?

- ☐ Sexting-ul desemnează acțiunea de a trimite fotografii nud/ aproape nud sau filmulețe cu un conținut sexual implicit cu minori.
- ☐ Sexting-ul traumatizează mii de adolescenți, afectându-le viața socială.

Unde are loc sexting-ul?

Sexting-ul se desfășoară în mediul virtual sau prin intermediul telefonului mobil.

Cum ar arăta un exemplu de sexting?

- ☐ Trimiterea de fotografii intime prietenului/nei cu care ești într-o relație, crezând că veți rămâne în spațiul privat.
- ☐ Minori determinați să se expună în ipostaze sexuale explicite în fața camerelor web de către persoane care folosesc identități fictive, pentru a putea fi înregistrați și ulterior șantajați sau minore determinate să producă materiale pornografice pentru prietenii lor, ulterior șantajate cu acestea.



III. LA CE PERICOLE MĂ EXPUN DACĂ **NU** FOLOSESC CORECT ȘI RESPONSABIL INTERNETUL?

Exemplu de sexting combinat cu cyberbullying:

„Un caz foarte mediatizat legat de acest ultim efect la nivel fizic al hărțuirii online este cazul Amandei Todd, adolescenta de 16 ani din Canada care, îndemnată de un necunoscut pe internet să își expună părțile intime, a ajuns să fie hărțuită de acesta constant, sub amenințarea că va posta poza cu ea dacă nu i se va supune. Adolescenta a refuzat cerințele agresorului, iar acesta a publicat fotografia cu ea, motiv pentru care a fost nevoită să se mute de la un liceu la altul, dintr-un oraș în altul, spre a ascunde rușinea.

Agresorul a continuat să o amenințe și să trimită poza ei către fiecare liceu unde se muta, iar fata a început să sufere de depresie, frică, atacuri de panică, a încercat să se automutileze și să se sinucidă, rezultatele școlare fiind din ce în ce mai slabe. În pofida terapiilor și tratamentului medicamentos la care a fost supusă, Amanda a fost găsită spânzурată în apartamentul ei, în octombrie 2012, nu înainte de a posta pe You Tube un clip video ce a devenit viral: „My Story: Struggling, bullying, suicide and self harm”, în care, folosindu-se de cartonașe, adolescenta povestește tragică sa experiență privind cyberbullyingul.

Filmul se poate viziona la adresa: https://www.youtube.com/watch?v=_gycqAJcDFM.

(„CYBER BULLYING – O PROBLEMĂ MAJORĂ FAVORIZATĂ DE UN CADRU LEGISLATIV DEFICITAR”)

Iulia-Laura Dobre, Elena Enăchescu

Cibernetică economică, An III, grupa 1056

Coordonator științific: Profesor Asociat Alina Mioara Cobuz-Băgnaru

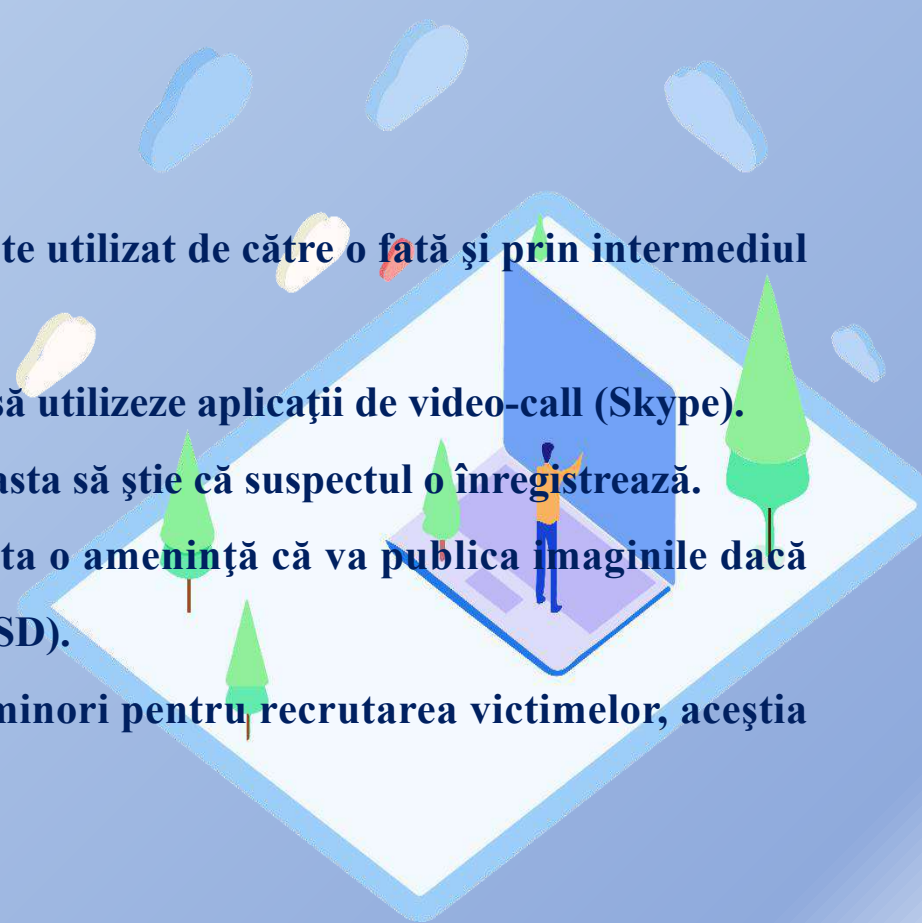
III. LA CE PERICOLE MĂ EXPUN DACĂ **NU** FOLOSESC CORECT ȘI RESPONSABIL INTERNETUL?

III.4. SEXTORTION

Suspectul folosește un cont pe rețelele sociale (ex: *Facebook*) ce aparent este utilizat de către o fată și prin intermediul căruia intră în contact cu potențiale victime de sex feminin.

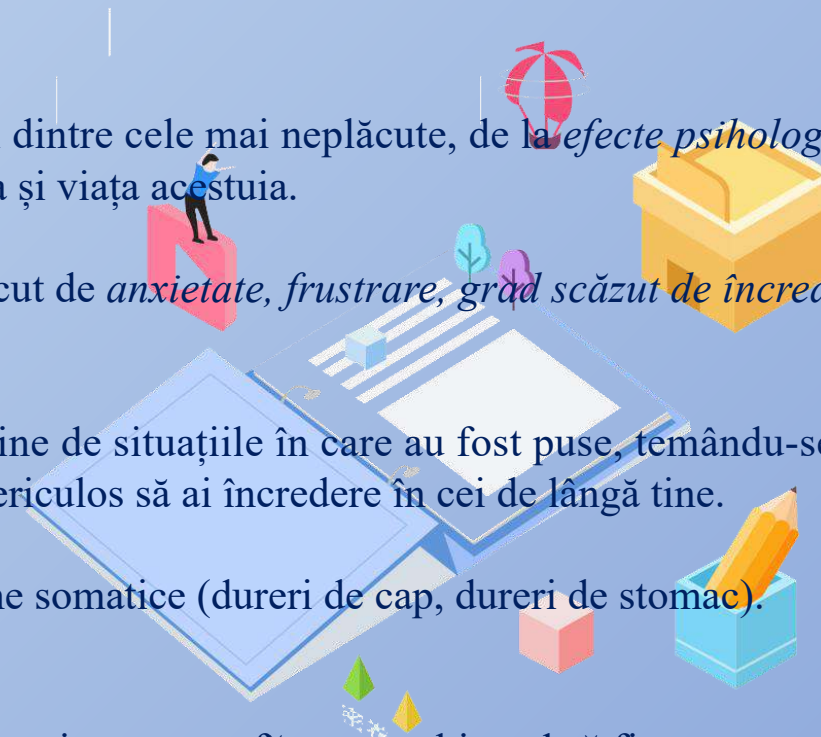
La scurt timp după ce începe să se cunoască cu victima, suspectul o invită să utilizeze aplicații de video-call (Skype). În timpul acestor conversații victima este convinsă să se dezbrace sumar, fără ca aceasta să știe că suspectul o înregistrează. Ulterior suspectul trimite mesaje pe contul de Facebook al victimei prin care acesta o amenință că va publica imaginile dacă aceasta nu va expedia o sumă de bani prin sistemul Western Union (în jur de 3000 USD).

Din investigațiile efectuate s-a stabilit că în unele cazuri au fost folosiți minori pentru recrutarea victimelor, aceștia primind în schimb sume de bani.



III.5. LA CE ALTE PERICOLE NE EXPUNEM DACĂ NU FOLOSIM CORECT ȘI RESPONSABIL INTERNETUL?

- ❑ Traumele copiilor care ajung victime ale agresiunilor din mediul virtual pot fi dintre cele mai neplăcute, de la *efecte psihologice*, la efecte care la rândul lor perturbă *viața socială* a copilului sau chiar sănătatea și viața acestuia.
- ❑ Numeroase studii au arătat corelația dintre victimizare pe internet și grad crescut de *anxietate, frustrare, grad scăzut de încredere în propriile forțe*.
- ❑ Pe plan social, victimele agresiunilor online ajung să se izoleze, fiindu-le rușine de situațiile în care au fost puse, temându-se că vor fi ținta unor ironii sau a oprobriului public și ajungând la concluzia că e periculos să ai încredere în cei de lângă tine.
- ❑ Există studii care arată inclusiv asocierea dintre victimizarea pe net și simptome somatice (dureri de cap, dureri de stomac).
- ❑ La nivel internațional, câteva cazuri de sinucideri ale unor adolescenți hărțuiți pe internet au făcut ca subiectul să fie tratat cu mai multă atenție și de instituții, dar și de părinți, profesori, societate în general .



III.5. LA CE ALTE PERICOLE NE EXPUNEM DACĂ NU FOLOSIM CORECT ȘI RESPONSABIL INTERNETUL?

❑ *Infectarea sistemelor cu programe de tip malware :*

- ✓ **Virusii** – reprezintă programe nedorite care se instalează singure în sistemul pe care îl atacă și pot provoca daune precum: distrugerea unor fișiere, ștergerea informațiilor, încetinirea vitezei de lucru a sistemului, ascunderea sau blocarea unor fișiere, multiplicarea fișierelor până la umplerea memoriei etc. Virusii se prezintă de obicei sub forma unor fișiere executabile atașate altor programe.
- ✓ **Viermii** – sunt programe cu efecte distructive cu capacități de automultiplicare ce se folosesc de rețele pentru a se răspândi. Spre deosebire de virusi, ei nu se atașează de programe pentru a se extinde și atacă direct sistemul, nu fișierele conținute de acesta. Simpla interconectare a unor sisteme în rețea face posibilă răspândirea viermilor.
- ✓ **Spyware** – programe-spion care se pot instala singure în sistem, care au capacitatea de a capta informații despre utilizator și de a le furniza celui care le-a creat și lansat. Programele spyware pot ajunge până la a oferi „beneficiarului” său control de la distanță asupra sistemului infectat prin sisteme de tip RAT – Remote Action Tool.

Infectarea cu malware, pe lângă riscul de disfuncționalitate a sistemului, aduce cu sine și alte riscuri: furtul de date și informații personale despre utilizator, parole de acces folosite de acesta pentru a accesa diverse site-uri sau aplicații, spionajul fizic(prin intermediul camerelor web ale sistemului).



III.5. LA CE ALTE PERICOLE NE EXPUNEM DACĂ NU FOLOSIM CORECT ȘI RESPONSABIL INTERNETUL?

❑ *Furtul de identitate*

Este definit, în general, ca fiind însușirea fără drept a datelor de identificare (nume, prenume, adresă, dată de naștere etc.) ale unei alte persoane, acest tip de risc este periculos nu atât în sine, prin însușirea fără drept a unei identități, cât prin folosirea ulterioară a acesteia. În contextul actual al evoluției criminalității, este deseori asociat cu infracțiunile legate de mijloacele de plată, în special cele electronice. Furtul de identitate în mediul virtual se poate face prin diferite metode, ca de exemplu:

- **Phishing** – este o formă de furt de identitate utilizat de obicei în legătură cu cardurile bancare și plățile online. Presupune transmiterea unor mesaje care atenționează utilizatorul asupra faptului că informațiile privind contul său de pe un anumit site au expirat, au fost compromise sau pierdute. Aceste mesaje apar ca fiind trimise din partea site-ului. Se solicită totodată transmiterea unui e-mail sau accesarea unui link care va fi redirectionat la un site fals (o clonă a întregului site original) unde i se solicită introducerea numărului cardului, a codului PIN și a altor date de identificare, după caz.
- **Pharming** – prin folosirea de programe malware, la încercarea de accesare a unor site-uri, redirectionează utilizatorii către domenii clonate ale paginii respective, de unde datele lor pot fi descărcate.



III.5. LA CE ALTE PERICOLE NE EXPUNEM DACĂ NU FOLOSIM CORECT ȘI RESPONSABIL INTERNETUL?

❑ *Dependența*

- utilizarea necontrolată, patologică a Internetului poate avea un impact negativ asupra performanțelor școlare, a relațiilor de familie și asupra stării emoționale a adolescenților, fiind un comportament cu semne și simptome similare cu cele ale oricărei alte dependențe. Pe lângă riscurile asociate unei adicții (izolare socială, probleme de sănătate cauzate de autonegligare, rezultate slabe și absențe la școală etc.) dependența de internet poate crește semnificativ riscul infectării calculatorului cu programe malware.



IV. CARE SUNT PAȘII PE CARE TREBUIE SĂ-I URMĂM ÎN CAZ DE PERICOLE, PENTRU A FI ÎN SIGURANȚĂ PE NET, DAR ȘI ÎN VIAȚA REALĂ?

1.

- ❑ În cazul în care o persoană cu care comunicați pe internet vă jignește, vă amenință, vă transmite mesaje cu tentă sexuală, vă cere să îi trimiteți poze cu voi sau vă trimite poze cu conținut pornografic, vă îndeamnă să consumați alcool ori droguri, *anunțați-vă părinții sau faceți o sesizare pe unul din site-urile specializate.*
- ❑ *Cereți ajutorul, în orice situație, persoanelor în care aveți încredere, părinți, profesori sau prieteni apropiați.*
- ❑ Dacă cineva vă face să vă simțiți inconfortabil pe Internet, puteți oricând să *renunțați la comunicarea cu acea persoană.* Nu sunteți obligați să stați pe Internet mai mult decât considerați voi și nici să suportați ceea ce vă provoacă neplăcere sau teamă; puteți oricând să îi *scoateți de pe lista de contacte pe cei cu care nu vreți să mai comunicați!*
- ❑ Sesizarea directă a organelor de poliție competente - *www.efrauda.ro, [cybercrime @politiaromana.ro](mailto:cybercrime@politiaromana.ro);*
- ❑ Solicitarea de sprijin ONG-urilor care gestionează website-uri în domeniu. Ex. *www.safernet.ro, www.oradenet.ro, www.116111.ro;*
- ❑ Orice situație de abuz asupra minorilor, petrecută în mediul online, trebuie *sesizată Poliției*, fie în mod direct, la cea mai apropiată unitate, fie prin intermediul Internetului, pe site-ul www.efrauda.ro.
- ❑ De asemenea, Organizația Salvați Copiii gestionează un help line destinat semnalărilor situațiilor de abuz sau agresiune pe internet, oferind și consiliere privind siguranța pe internet, pentru copii și părinți.

IV. CARE SUNT PAȘII PE CARE TREBUIE SĂ-I URMĂM ÎN CAZ DE PERICOLE, PENTRU A FI ÎN SIGURANȚĂ PE NET, DAR ȘI ÎN VIAȚA REALĂ?

2.

Ne adresăm

CENTRULUI JUDEȚEAN DE RESURSE ȘI ASISTENȚĂ EDUCAȚIONALĂ

„Te afli într-o situație în care emoțiile sunt atât de puternice încât te împiedică să întrevezi o rezolvare, te simți vulnerabil, ești dezorientat, ai probleme de adaptare, de relaționare sau traversezi o perioadă dificilă, de derivă, de separare, izolare, încărcată de presiuni profesionale, sociale, stres?”

Iată o soluție:

*Contactează-ne la numărul de telefon **0752/099 366** și vei fi pus în legătură cu un profesor consilier școlar din cadrul Centrului Județean de Resurse și Asistență Educațională Arad care îți poate oferi susținere și te poate ajuta să găsești răspunsuri și soluții la experiențele pe care le trăiești.”*

(Echipa C.J.R.A.E. Arad)

3.

Ne adresăm

ASOCIAȚIEI TELEFONUL COPILULUI

„Pentru mulți dintre voi, necunoscutul și schimbarea sunt principalele provocări pe care carantina sau autoizolarea le-au adus în viața voastră. Știm că vă este greu și pentru că nimeni nu știe și nu vă poate spune cât de mult poate să dureze pandemia și ce urmează să se întâmple în timp ce vouă vă este dor de viața de dinainte de pandemie, de toate planurile pe care acum nu vi le puteți duce la bun sfârșit.

Ne puteți suna la 116 111, ne puteți scrie direct pe www.116111.ro sau în chat-ul aplicației Happygraff pentru a afla cum puteți face față acestei perioade teribile și cum să vă concentrați pe ceea ce puteți controla acum.

Anonim & confidențial!”

(Mesaj din partea Asociației Telefonul copilului)

**ȘTIM CĂ LUMEA PARE CĂ
S-A OPRIT ÎN LOC, DAR NOI
SUNTEM TOT AICI!**

**SUNĂ-NE LA 116 111 SAU SCRIE-NE
DIRECT PE WWW.116111.RO.**

**SUNTEM ȘI ÎN CHATUL
APLICAȚIEI HAPPYGRAFF
(DIN GOOGLE PLAY)**



#116111

#WWW.116111.RO

#HAPPYGRAFF

@ASOCIATIA TELEFONUL COPILULUI

IV. CARE SUNT PAȘII PE CARE TREBUIE SĂ-I URMĂM ÎN CAZ DE PERICOLE, PENTRU A FI ÎN SIGURANȚĂ PE NET, DAR ȘI ÎN VIAȚA REALĂ?

4.

DIRECȚIA GENERALĂ DE ASISTENȚĂ SOCIALĂ ȘI PROTECȚIA COPILULUI

„Pentru sesizarea situațiilor în care sănătatea și siguranța unui copil este pusă în pericol, Direcția Generală de Asistență Socială și Protecția Copilului Arad (D.G.A.S.P.C.) dispune de un serviciu specializat - **TELEFONUL DE URGENTĂ - ECHIPA MOBILĂ**.

Trebuie știut faptul că numărul de telefon **0257 -983** poate fi apelat în orice moment al zilei, de orice persoană care dorește să semnaleze cazuri de copii abuzați, neglijăți, aflați în situație de risc sau în dificultate, situații de abuz fizic, emoțional, sexual, neglijare și exploatare a copilului, a victimei violenței în familie.”

(Echipa D.G.A.S.P.C. Arad)

IV. CARE SUNT PAȘII PE CARE TREBUIE SĂ-I URMĂM ÎN CAZ DE PERICOLE, PENTRU A FI ÎN SIGURANȚĂ PE NET, DAR ȘI ÎN VIAȚA REALĂ?

„Școala să nu fie nimic altceva, decât ateliere pline de activitate. Numai astfel vor putea să probeze toți, în propria lor practică, adevărul că: învățând pe alții ne învățăm pe noi înșine”.

John Amos Comenius

