



COLEGIUL NAȚIONAL
PETRU RAREȘ
ȘCOALĂ EUROPEANĂ



BECLEAN, Strada Obor, nr. 83
JUDEȚUL BISTRIȚA-NĂSAUD
Tel/Fax: 0363566910/0363566909
Web: <http://www.cnpruraresbn.ro/>
E-mail: cnprbeclean@yahoo.com

Nr. 3599/08.09.2025

POLITICA DE UTILIZARE ACCEPTABILĂ (E-SAFETY) A COLEGIULUI NAȚIONAL „PETRU RAREȘ” BECLEAN



Director,
Prof. POP CRISTIAN

Director adjunct,
Prof. CÎMPEAN MARIKA EMESE



POLITICA DE UTILIZARE A RESURSELOR ONLINE ÎN ACTIVITĂȚILE ȘCOLARE ȘI EXTRAȘCOLARE

Art. 1 Orele de tehnologia informației și a comunicațiilor (TIC) și informatică prevăzute în curriculum se desfășoară, de regulă, în cabinetele de informatică ale școlii sub supravegherea profesorului de specialitate.

Art. 2 Tot în vederea dezvoltării competențelor digitale ale elevilor și a personalului didactic, la alte discipline, profesorii, împreună cu elevii, pot desfășura activitatea de predare-învățare-evaluare în laboratoarele de informatică, în cabinetele de specialitate sau în săli de clasă prevăzute cu laptop și videoproiector.

Art. 3 Folosirea instrumentelor TIC permite elaborarea și implementarea metodelor moderne de predare-învățare. Astfel, în timpul orelor, elevii au ocazia de a viziona filmulețe, prezentări, documente, imagini care fac orele mai atractive decât mijloacele tradiționale cum ar fi tabla sau manualul.

Art. 4 În timpul accesării platformelor educaționale sau a altor site-uri necesare activităților educative, elevii vor respecta indicațiile profesorului, intrând doar pe site-urile permise, considerate sigure din punct de vedere al virușilor cibernetici.

POLITICA DE SIGURANȚĂ ONLINE

Art. 1 Majoritatea platformelor educaționale folosite în activitatea didactică sunt securizate și verificate în prealabil, astfel încât materialele postate (fișiere, imagini) sunt private.

Art. 2 Fotografii în care apar elevi vor rămâne doar pe platforma educațională și nu vor fi utilizate în alte scopuri (de exemplu în prezentări sau alte site-uri), decât cu acordul acestora.

Art. 3 Pentru a proteja elevii de orice formă de abuz, aceștia vor fi instruiți periodic la orele de TIC și dirigenție referitor la pericolele la care se pot expune folosind diverse resurse online. Elevii vor raporta profesorului sau coordonatorului eSafety dacă primesc amenințări directe, sunt intimidați sau hărțuiți sau dacă primesc mesaje care incită la ură, rasism, violență.

Art. 4 Materialele încărcate pe platforme educaționale (imagini, videoclipuri, documente etc.) trebuie să respecte drepturile de autor. De pe Internet se pot folosi doar fotografiile destinate utilizării comerciale cu titlu gratuit.

Art. 5 În activitățile desfășurate de profesori împreună cu elevii pe platformele educaționale, profesorii se vor preocupa de confidențialitatea și siguranța elevilor - vor evita să pună numele întreg al elevilor, să publice fotografiile ale elevilor în profilul lor decât dacă identitatea acestora va fi nerecognoscibilă sau vor avea acordul părinților.



Art. 6 Conținuturile publicate nu vor divulga informații personale sau date sensibile, cum ar fi: adrese, numere de telefon, etc.

POLITICA LEGATĂ DE UTILIZAREA DISPOZITIVELOR/TELEFOANELOR MOBILE

Art. 1 În timpul orelor de curs telefoanele mobile ale elevilor se păstrează în locul special amenajat în acest scop în sălile în care acesta există sau în ghiozdane. Pe timpul pauzei, elevii le iau în grija personală.

Art. 2 Elevii pot utiliza telefonul în timpul orei de curs doar în scop instructiv - educativ, numai la solicitarea cadrului didactic, dacă acesta consideră că este necesar.

Art.3 Elevii nu pot accesa rețeaua WiFi a școlii prin intermediul telefoanelor mobile.

Art. 4 Este interzis elevilor, precum și personalului școlii, să consulte conținut pornografic sau ilegal în timp ce sunt la școală.

Art. 5 Telefonul elevilor poate fi confiscat de către cadrul didactic în timpul orei de curs dacă acesta nu respectă prevederile articolelor anterioare. În acest caz, elevul trebuie să oprească telefonul înainte de a-l înmâna profesorului, pentru a asigura protecția datelor personale de pe telefon. Telefonul va fi returnat la sfârșitul orelor de curs.

POLITICA PRIVIND FOTOGRAFIEREA / FILMAREA

Art. 1 Activitățile școlare și extrașcolare sunt evenimente ce prilejuiesc motive de mândrie. Pentru a fi momente de neuitat, acestea se pot fotografia sau filma și păstra în biblioteca școlii.

Art. 2 Înainte de a se desfășura evenimente școlare, elevii vor fi anunțați că la acel eveniment se va filma sau fotografia, cerându-li-se permisiunea. Dacă un elev/un părinte nu își dă acordul, acesta va fi omis.

Art. 3 Este interzisă postarea numelui complet, vârsta sau orice alte detalii personale alături de fotografia unui copil pe site-ul unui profesor sau al colegiului.

POLITICA DE FOLOSIRE A DISPOZITIVELOR DE STOCARE EXTERNA

Art. 1 Protecția antivirus/firewall este instalată și actualizată constant.

Art. 2 Personalului și elevilor li se cere să scaneze pentru viruși orice dispozitiv de stocare extern atunci când îl folosesc pe un computer al școlii.

Art. 3 Personalul nu salvează date sensibile pe dispozitive de stocare externa.



Anexe:

- Anexa 1. Angajament de conformare/Declarație de luare la cunoștință a politicii eSafety a CNPR Beclean
- Anexa 2. Politica de utilizare acceptabilă (elaborată de European Schoolnet)
- Anexa 3. Chestionar de autoevaluare „E-safety pentru instituții de învățământ”, (Ora de Net/Salvați Copiii)
- Anexa 4. Caietul de lucru „Ne jucăm și învățăm: Navigarea pe Internet” (publicația de European Schoolnet)
- Anexa 5. Broșura „Smartphone: imaginea ta online” (Salvați Copiii)
- Anexa 6. Kitul de acțiune pentru adolescenți: „Spune-ți părerea despre drepturile tale online!”



Anexa 1 la POLITICA DE UTILIZARE ACCEPTABILĂ (E-SAFETY) A COLEGIULUI NAȚIONAL „PETRU RAREȘ” BECLEAN

ANGAJAMENT DE CONFORMARE

Confirm faptul că:

- am luat la cunoștință despre prevederile POLITICA DE UTILIZARE ACCEPTABILĂ (E-SAFETY) A COLEGIULUI NAȚIONAL „PETRU RAREȘ” BECLEAN;
- am participat la programele de pregătire și am fost instruit conform prevederilor Regulamentului COLEGIULUI NAȚIONAL „PETRU RAREȘ” BECLEAN privind politica de utilizare acceptabilă (eSafety) a Colegiului Național „Petru Rareș” Beclean.

Înțeleg că am obligația de a respecta dispozițiile legale privind utilizarea acceptabilă a TIC, în concordanță cu etosul școlii, cu alte politici adecvate și cu legea, în calitate de salariat al COLEGIULUI NAȚIONAL „PETRU RAREȘ” BECLEAN.

Îmi asum personal responsabilitatea pentru respectarea integrală a principiilor, cerințelor și obligațiilor care rezultă din dispozițiile legale privind utilizarea responsabilă și Regulamentul COLEGIULUI NAȚIONAL „PETRU RAREȘ” BECLEAN privind siguranța online, elaborat în aplicarea prevederilor legale specifice.

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

Subsemnatul/subsemnata _____,
domiciliul _____, data nașterii _____,
în calitate de _____, în cadrul
COLEGIULUI NAȚIONAL „PETRU RAREȘ” BECLEAN, am citit și înțeles și sunt de acord
cu respectarea POLITICII DE UTILIZARE ACCEPTABILĂ A TIC de către personalul angajat
al COLEGIULUI NAȚIONAL „PETRU RAREȘ” BECLEAN.

Am fost informat că datele cu caracter personal sunt prelucrate în scopul și pentru îndeplinirea atribuțiilor legale ale instituției.

Am luat la cunoștință că informațiile din cererea depusă și din actele anexate la aceasta, vor fi prelucrate de instituție cu respectarea prevederilor Regulamentului (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, și libera circulație a acestor date.

Data

Semnătura angajatului:

ESAFETYLABEL.EU



For safer schools!

Politica de Utilizare Acceptabilă (PUA)

POLITICA eSAFETY A ȘCOLII COLEGIUL NAȚIONAL „PETRU RAREȘ” BECLEAN

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

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

UTILIZAREA TELEFOANELOR MOBILE ÎN ȘCOLI

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



- Rețeaua Wi-Fi a școlii nu este accesibilă pe telefoanele mobile, dar poate fi accesată de către elevi, pe cea separată de rețeaua securizată destinată personalului / activităților principale (router wi-fi instalat în clasă).
- În cazul confiscării unui telefon mobil, elevul trebuie să oprească telefonul înainte de a-l înmâna profesorului, pentru a asigura protecția datelor personale de pe telefon. Dacă telefonul nu este returnat la sfârșitul orelor de curs, părinții ar trebui să fie informați și telefonul mobil trebuie să fie păstrat într-un loc sigur .
- Părinții sunt informați cu privire la politica referitoare la utilizarea telefonului mobil, cu privire la motivele pentru care sunt luate aceste măsuri și cu privire la posibilele consecințe pe care le poate implica o încălcare a acestei politici.

UTILIZAREA DISPOZITIVELOR DETAȘABILE

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

- În cadrul Politicii de Utilizare Acceptabilă sunt dezvoltate reguli de bază privind folosirea dispozitivelor detașabile de stocare pe computerele școlii.
- Este instalat un sistem de protecție antivirus pe toate computerele din rețeaua școlară și se adoptă o practică constantă la nivel de școală în ceea ce privește protecția împotriva virușilor. Un fișier infectat de pe un dispozitiv de stocare amovibil ar putea infecta întreaga rețea școlară.
- Se solicită membrilor personalului și elevilor să scaneze toate dispozitivele detașabile împotriva programelor malware înainte de a le utiliza.
- Se permite utilizarea dispozitivelor mobile numai când sunt necesare în vederea îndeplinirii sarcinilor școlare. Elevilor și membrilor personalului nu trebuie să li se permită, de exemplu, să-și conecteze aparatul foto sau un MP3 player-ul la un computer din rețeaua școlii, cu excepția cazului în care trebuie să facă acest lucru în cadrul unei sarcini specifice pe care au primit-o.
- Se încurajează personalul și elevii să salveze fișiere pe dispozitivele mobile pe care le folosesc pe computerele școlii doar în scopuri educaționale .
- Personalul trebuie să evite stocarea datelor sensibile ale elevilor și ale altor membri ai personalului pe dispozitive detașabile cu excepția cazului în care acest lucru este



necesar în vederea executării sarcinilor ce le revin, deoarece există întotdeauna riscul ca aceste dispozitive cu informații personale pe ele să fie furate sau pierdute.

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

PROTEJAREA DATELOR SENSIBILE ÎN ȘCOLI

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

- Se actualizează sistemele de protecție antivirus pentru a evita să deveniți o țintă a hackerilor.
- Inginerie socială ¹ reprezintă cel mai mare risc de securitate; se discută cu personalul din școală pentru asigurarea că aceștia nu se lasă păcăliți în oferirea de date.
- Nu lăsați documente ce conțin date sensibile pe imprimanta publică sau salvate pe calculator! Distrugeți / stergeți astfel de documente înainte să le puneți în coșul de gunoi (Recycle Bin).
- Colectați date sensibile doar dacă este necesar. Ceea ce nu deții, nu poate fi compromis!

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

PROTECȚIA DISPOZITIVELOR ÎMPOTRIVA

PROGRAMELOR MALWARE

Malware înseamnă software dăunător care a fost proiectat cu scopul accesării unei rețele sau unui sistem de calculare fără consimțământul proprietarului și poate include viruși, viermi și spyware. Odată instalat, malware-ul cauzează de obicei rezultate nedorite, care pot varia de la a fi pur și simplu intruziv sau enervant până la a compromite informații cu caracter personal în sistem sau până la a fi pur și simplu distructiv. Malware-ul ajunge de obicei în sistemul IT al unei școli prin intermediul spam-ului, descărcării de fișiere



contaminate sau prin intermediul dispozitivelor mobile infectate (USB, hard disk extern, telefon mobil, etc.).

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

POLITICA DE UTILIZARE ACCEPTABILĂ (PUA)

Reprezintă o bună practică ca toate școlile să aibă o Politică de Utilizare Acceptabilă (PUA), adică un document clar și concis care să ofere îndrumare unor categorii de utilizatori cu privire la felul în care ar trebui utilizate Internetul și tehnologiile mobile.

Politicile de Utilizare Acceptabilă s-au dezvoltat în timp și este evident că tinerii și personalul din școli au posibilitatea să acceseze Internetul în multe moduri, nu numai prin intermediul rețelei școlii. Având în vedere acest fapt, este important ca o Politică de Utilizare Acceptabilă să fie centrată mai mult pe comportament decât pe tehnologie. Acest lucru înseamnă că politica va avea o viață mai lungă și va fi mai ușor de înțeles de către toți cei interesați.

PAROLE SIGURE

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

- Se amintește personalului și elevilor cele 4 reguli de aur ale unui parole sigure:
 1. Trebuie să fie lungă și complexă. Ideal trebuie să conțină între 10 și 14 caractere ;
 2. Se folosește un amestec de numere, simboluri, litere mari și litere mici și semne de punctuație ;



3. Se folosește metode mnemonice care să vă ajute să vă amintiți parola, de exemplu un acronim pentru o frază, cum ar fi "Fiica mea, Harriet, este o bună jucătoare de tenis" devine FMhEObjDt sau Imi place să cânt in ploaie in fiecare zi! devine iPScipIFZ !;
4. Nu folosiți niciodată informații personale de identificare în parolă. Acestea includ nume, zile de naștere, animale de companie, adrese de străzi, școli, numere de telefon, numerele de înmatriculare etc. Acestea vor fi primele presupuneri pentru oricine încearcă să obțină acces la contul dvs.
 - O parolă este ca o periută de dinți, nu trebui folosită în comun și trebuie să fie schimbată frecvent!
 - Dacă utilizatorii simt totuși nevoie să scrie parola, aceasta nu trebuie să fie ținută în apropierea dispozitivului la care oferă acces.

POLITICA ȘCOLII

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

REALIZAREA ȘI PUBLICAREA DE FOTOGRAFII ȘI CLIPURI

VIDEO ÎN CADRUL ȘCOLII

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

- Se asigură că școala are o politică clară referitoare la imagine și fotografie indiferent dacă aceasta este sau nu o obligație legală în țara dvs.
- Se comunică comunității școlare această politică alături de îndrumări practice clare și exemple ușor de înțeles.
- Se asigură că toți părinții/tutorii legali și/sau tinerii (în funcție de vârstă și cerințe naționale) au semnat un formular de permisiune pentru foto/video ÎNAINTE de orice filmare sau fotografiere a elevilor.



- Dacă părintele/tutorele nu-și dă acordul, înțelegeți posibilul disconfort al elevului respectiv și aranjați discret ca el/ea să aibă o altă ocupație în timpul procesului de filmare sau fotografiere.
- Se asiguraă că toți membri comunității școlare înțeleg implicațiile partajării fotografiilor și conținutului video pe site-urile de socializare – nu postați NICIODATĂ numele complet, vârsta sau orice alte detalii personale alături de fotografia unui copil pe site-ul dvs.!
- Țineți minte că evenimentele școlare sunt ocazii de bucurie care nu ar trebui să fie restricționate de prea multe reglementări.

PREZENȚA ȘCOLII PE REȚELELE DE SOCIALIZARE

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

Pe lângă rolul de instrument promoțional pentru școli, profesorii din toată lumea au enumerat mai jos beneficiile utilizării rețelelor sociale în școli.

- Dezvoltarea profesională în ceea ce privește utilizarea instrumentelor tehnice și de social media pentru profesori.
 - Utilizarea unor metode de învățare moderne, incluzive și alternative.
 - Informarea și sensibilizarea comunității și a părinților prin intermediul grupurilor de Facebook, Pinterest, Yammer, Twitter și altele.
 - Comunicarea cu părinții în cazul în care sunt prieteni pe Facebook cu școala/clasa/proiectul școlar.
 - Comunicarea interculturală cu alte școli.
 - Învățarea limbilor străine.
 - Învățarea colaborativă și împărtășirea de informații cu colegi și grupuri educaționale cu aceleași interese.
 - Stabilirea de legături cu colegi din întreaga țară și chiar din lume.
 - Integrarea unor exemple din lumea reală în procesul de predare.
- ✓ **Rețeaua de socializare Facebook este restricționată în sălile de clasă unde se desfășoară orele de curs.**



INTEGRAREA ESAFETY ÎN CURRICULUM

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

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

INFORMAȚII PENTRU PĂRINȚI

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

- Școlile trebuie să ofere sprijin, îndrumare și consiliere pentru părinți. Acest lucru poate lua diverse forme, o discuție specifică pe această temă, pliante despre diferite probleme, legături (link-uri) pe site-ul școlii sau un articol în buletinul online al școlii.
- Este important să recunoaștem că de multe ori părinții care participă la o seară eSafety sunt tocmai părinții care probabil nu au nevoie să participe! Părinții interesați de ceea ce



fac copiii lor vor fi, de asemenea, mult mai conștienți cu privire la problemele cu care aceștia se confruntă online și vor fi dornici să comunice pe aceste teme.

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

UTILIZAREA TEHNOLOGIEI ONLINE DE CĂTRE

ELEVI ÎN AFARA ȘCOLII

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

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

GESTIONAREA INCIDENTELOR

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



- Este important să se revizuiască incidentele la ședințele periodice cu personalul. Rețineți că imediat după incident ar putea exista o rezistență firească la revizuirea incidentului din partea membrilor personalului implicat. Lăsați să treacă un timp, astfel încât toată lumea să privească incidentele cu detașare.
- Discutați întrebările din lista de control eSafety atunci când revizuiți un incident.
- Raportați incidentul prin intermediul [incident handling report](#). Raportarea incidentelor prin intermediul unui șablon furnizat pe site va conta în acordarea punctelor de acreditare, va rămâne anonimă și ne va ajuta pe toți să învățăm unii de la alții.

CYBERBULLYING

Cyberbullying – denumit uneori și bullying online; este o problemă foarte complexă. Poate fi definit ca utilizarea tehnologiei și în special a telefoanelor mobile și Internetului, pentru a răni în mod deliberat, supăra, hărțui sau a jena o persoană. Acesta poate fi prelungire a intimidării față-în-față, tehnologia oferind agresorului o altă metodă de hărțuire a victimei, sau fără niciun motiv. Poate avea loc prin intermediul oricărei forme de media, de la mesaje și imagini ofensatoare trimise de pe telefoane mobile, la postări neplăcute pe bloguri și pe rețelele de socializare sau e-mailuri și mesagerie instantanee, până la site-uri dăunătoare create numai cu scopul de a intimida o persoană sau abuz virtual în timpul unui joc multiplayer online. Cyberbullying-ul diferă de alte forme de bullying; poate invada casa și spațiul personal al victimei, publicul este potențial mai numeros, mesajele sau imaginile supărătoare pot fi propagate rapid și există dificultăți în controlarea și/sau eliminarea mesajelor transmise electronic. De asemenea, deoarece nu presupune interacțiune față-în-față, cyberbullying-ului i se atribuie de obicei un caracter anonim. Acest lucru îi poate determina pe oameni să se implice în activități în care nici n-ar visa să se implice în lumea reală, fie ca autor sau ca un spectator.

- Se adoptă o abordare anti-bullying la nivelul întregii școli.
- Comunicați în mod clar strategia pentru toți membrii comunității școlare - elevi, cadre didactice, personal adițional și părinți. Toată lumea ar trebui să fie conștientă de traseele de raportare și de consecințele pentru cei implicați în astfel de comportamente.
- Se revizuieste periodic strategia adoptată, se evaluează succesul acesteia și adaptați-o dacă este necesar.
- Organizați sau încurajați formări pentru profesori.
- Integrați în programă conștientizarea cu privire la (cyber) bullying pentru toate categoriile de vârstă. - Organizați sesiuni de informare pentru părinți. Aceștia ar putea să nu fie conștienți de noile instrumente tehnologice și de modul în care copiii lor le folosesc.



ASPECTE LEGALE ALE PROTECȚIEI DATELOR

Protecția vieții private și a datelor cu caracter personal ale tuturor elevilor și personalului din școală este reglementată de legislația națională din țara dvs. privind protecția datelor. Deși aceste reguli se bazează pe o Directivă Europeană ([95/46/EC](#)) există multe diferențe în modul în care țările au transpus acest document în legislația națională. Pentru a ști ce reguli se aplică în țara dumneavoastră consultați site-ul [national Data Protection Authority](#). (<http://ec.europa.eu/justice/data-protection/bodies/>)

În 2012, Comisia Europeană a propus o reformă majoră a Directivei Europene pentru Protecția Datelor. Noile propuneri vor consolida drepturile individuale și vor aborda provocările globalizării și noilor tehnologii. Puteți urmări discuțiile și deciziile referitoare la această nouă propunere pe [EC website](#) (http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm) și descoperiți ce implicații ar putea avea acest lucru asupra protecției confidențialității și a datelor cu caracter personal în școala dvs.

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

Am citit și înțeles și sunt de acord cu respectarea Politicii de Utilizare Acceptabilă a TIC de către personal.

Semnătură: Nume: Dată:

Acceptat de: Nume:



Anexa „Chestionar autoevaluare E-safety pentru instituții de învățământ”

COMPONENTA DATE PERSONALE

1. Lista de verificare: Aspecte legale ale protecției datelor Facem acest lucru în școala noastră?

	Da	Parțial	Nu
Politică			
1. Avem un protocol aplicat în mod riguros în ceea ce privește descărcarea/trimiterea/printarea și stocarea datelor cu caracter personal.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. Menținem o legătură strânsă cu persoana de contact din cadrul Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal. ¹	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Practică			
3. Organizăm sesiuni de formare pentru angajații noștri susținute de o persoană specializată.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4. Organizăm anual cel puțin o întâlnire cu membrii personalului pentru a discuta despre importanța protecției datelor cu caracter personal.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

COMPONENTA PRACTICI E-SAFETY

1. Listă de verificare: Integrarea eSafety în curriculum Facem acest lucru în școala noastră?

	Da	Parțial	Nu
Infrastructură			
1. Deși infrastructura noastră TIC este suficient de securizată, iar accesul la internet este filtrat, acest lucru nu limitează capacitatea elevilor noștri de a explora multitudinea de oportunități online.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Politică			
2. Politicile școlii se referă în mod explicit la integrarea eSafety în programă, astfel încât toți profesorii noștri au luat la cunoștință această responsabilitate comună.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Practică			
3. eSafety se predă ca parte a programei.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4. Toate cadrele didactice beneficiază de formare periodică eSafety.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5. Elevii se monitorizează reciproc pe probleme legate de eSafety.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6. Școala oferă sprijin eSafety pentru elevi în afara programei.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

¹ Puteți găsi detaliile despre persoana de contact din țara dumneavoastră la adresa:

http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm

2. Listă de verificare: Cursuri de formare eSafety
Facem acest lucru în școala noastră?

	Da	Parțial	Nu
Politică			
1. Este cunoscută și înțeleasă PUA de către toți membrii personalului?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. Personalul este informat regulat, cel puțin anual, cu privire la problematica eSafety	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. eSafety face parte din instructajul introductiv oferit noilor membrii ai personalului.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Practică			
4. Întreg personalul a beneficiat de formare eSafety în ultimele 12 luni.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5. Există un program planificat de formare eSafety orientat spre diferite categorii de personal.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6. Formarea profesională continuă este actualizată și face referire la trenduri și aspect ce țin de eSafety.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7. Formarea eSafety este realizată de către un trainer specializat pe domeniul siguranței online.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

3. Listă de verificare: Cyberbullying
Facem acest lucru în școala noastră?

	Da	Parțial	Nu
Infrastructură			
1. Utilizează școala noastră o tehnologie de monitorizare a rețelei informatice care semnalează cuvinte cheie sau limbaj inadecvat ce poate fi asociat cu bullying-ul? (Amintiți-vă totuși că asemenea activități au loc de obicei în afara rețelei școlii și în afara orelor de curs.)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. Există în școala noastră o persoană (probabil un membru în cadrul echipei educaționale) responsabilă cu supravegherea tuturor problemelor legate de bullying? (Această persoană va avea rolul de punct de contact pentru raportări și sfaturi, va fi capabilă să recunoască tendințele și va fi responsabilă cu revizuirea și modificarea periodică a tuturor politicilor relevante)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. Oferă școala noastră posibilitatea raportării anonime a incidentelor legate de bullying?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Politică			
4. Există o politică anti-bullying la nivelul întregii școli?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5. Include această politică incidente de cyberbullying care pot lua naștere în afara școlii și metode de răspuns la asemenea incidente?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6. Oferim în clasă și în școală un mediu care să încurajeze comportamentul pozitiv și sprijinul între colegi?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- | | | | |
|--|--------------------------|--------------------------|--------------------------|
| 7. Este întreaga comunitate (personal, elevi și părinți) conștientă de reguli și de consecințele bullying-ului? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 8. Este politica anti-bullying revizuită și întărită periodic pentru a vedea dacă sunt necesare adaptări (de exemplu, în cazul unor noi tehnologii sau descoperiri)? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Practică

- | | | | |
|---|--------------------------|--------------------------|--------------------------|
| 9. Beneficiază întregul personal de formare periodică cu privire la caracteristicile bullying-ului on și offline și la metodele adecvate de răspuns în acest tip de situații? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 10. Primesc elevii de toate vârstele informații cu privire la cyberbullying și la modalitățile de căutare a sprijinului și sfaturilor? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 11. Folosește școala noastră strategii de implicare a părinților în chestiunile legate de bullying și cyberbullying (ex. seri de informare, sfaturi pe site-ul școlii)? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 12. Avem procedure implementate care să ofere sprijin părinților care întâmpină acasă dificultăți legate de cyberbullying? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

4. Listă de verificare: Utilizarea tehnologiei de către elevi în afara școlii

Facem acest lucru în școala noastră?

Da Parțial Nu

Politică

- | | | | |
|--|--------------------------|--------------------------|--------------------------|
| 1. Politica noastră de utilizare acceptabilă include informații despre cum sunt gestionate problemele online care au loc în afara școlii. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2. În cazul unor probleme serioase, profesorii sunt aglibași să informeze părinții și să ceară ajutorul unor experți externi atunci când este necesar. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Practică

- | | | | |
|---|--------------------------|--------------------------|--------------------------|
| 3. Părinții și elevii sunt informați cu privire la angajamentul școlii în ceea ce privește aceste aspecte. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 4. Activități de conștientizare pe tema siguranței online sunt organizate cel puțin o dată pe an. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 5. Formarea personalului pe teme ce țin de siguranța online este organizată anual. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 6. Am desemnat un profesor sau consilier la care elevii pot apela în cazul în care întâmpină probleme online. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

5. Listă de verificare: Sexting
Facem acest lucru în școala noastră?

	Da	Parțial	Nu
Politică			
1. Este sextingul și abordarea școlii inclusă în politica de protecție a copilului?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. Face politica noastră referire la rolul școlii în incidente care au loc în exterior ex. atunci când elevii nu sunt la școală?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. Sunt elevii conștienți de consecințele împărtășirii imaginilor de tip sexting – atât din punctul de vedere al școlii, cât și din perspectiva legii?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4. Sunt referințele la sexting actualizate constant pentru a reflecta schimbările din legislație, practice curente și sfaturile oferite școlilor?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Practică			
5. Primesc membrii relevanți ai personalului formare cu privire la caracteristicile fenomenului de sexting și abordarea școlii? Știu acestia cum să gestioneze incidentele?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6. Primesc elevii informații despre cum să gestioneze situațiile de sexting și unde să ceară îndrumare sau ajutor?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7. Are școala noastră implementate strategii despre cum să informeze părinții cu privire la fenomenul de sexting (ex. întâlniri cu părinții, informații pe website-ul școlii)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8. Avem implementate sisteme de suport pentru părinții care întâmpină dificultăți legate de fenomenul de sexting în afara școlii?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

6. Listă de verificare: Extremism online, radicalizare și discurs instigator la ură
Facem acest lucru în școala noastră?

	Da	Parțial	Nu
Politică			
1. Sunt riscurile legate de extremism online și radicalizare menționate în politica de protecție a copilului?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. Face referire politica la rolul școlii în incidente ce au loc în afara, ex. atunci când elevii nu sunt la școală?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. Sunt elevii și profesorii informați cu privire la abordarea școlii privind discursul instigator la ură?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4. Sunt referințele la extremismul online și radicalizare actualizate în mod regulat astfel încât să reflecte schimbările din lege, practicile actuale și sfaturile oferite în școală?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Practică			
5. Primesc toți membrii personalului training în mod regulat referitor la riscurile radicalizării? Știu toți să recunoască potențialele probleme? Știu ce să facă în cazul în care au îngrijorări cu privire la un elev?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6. Primesc elevii informații despre cum să se protejeze de extremism online și radicalizare?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- | | | | |
|--|--------------------------|--------------------------|--------------------------|
| 7. Are școala implementate strategii de a discuta cu părinții despre probleme legate de extremism online și radicalizare (ex. Informații pe website, întâlniri cu părinții)? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 8. Avem proceduri implementate care să ofere sprijin părinților care întâmpină dificultăți în a înțelege extremismul online și radicalizarea în afara școlii? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 9. Există oportunități de prezentare a unor contra-narative la discursul instigator la ură și extremism online prin curriculum? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

7. Listă de verificare: Gestionarea incidentelor

A gestionat personalul școlii în mod corect incidentul?

	Acțiune necesară	Totul este în regulă	Comentariu
Procesul general			
Conține Politica Școlii o procedură de gestionare a incidentelor cunoscută de întregul personal? Sunt incluse numerele de telefon pentru liniile de asistență? Poate fi îmbunătățită procedura actuală în lumina acestui incident?	<input type="checkbox"/>	<input type="checkbox"/>	
A știut toată lumea cum să gestioneze incidentul? În cazul în care părțile implicate, de exemplu părinți, poliție, etc. au trebuit implicate/informate, a fost făcut acest lucru în mod corect și la timp?	<input type="checkbox"/>	<input type="checkbox"/>	
Ar fi fost posibil ca incidentul să fie descoperit mai devreme?	<input type="checkbox"/>	<input type="checkbox"/>	
Incidente privind accesul neadecvat			
Există o persoană numită responsabil cu monitorizarea regulată a serviciilor?	<input type="checkbox"/>	<input type="checkbox"/>	
Are școala noastră toate datele sensibile stocate pe un server separat la care are acces doar personalul autorizat?	<input type="checkbox"/>	<input type="checkbox"/>	
Suntem conștienți de noile „găuri” de securitate pe măsură ce acestea devin cunoscute și aplicăm soluții corespunzătoare?	<input type="checkbox"/>	<input type="checkbox"/>	
Este personalul nostru conștient de importanța securizării datelor sensibile cu parole sigure?	<input type="checkbox"/>	<input type="checkbox"/>	
Incidente privind bullying-ul			
Există o persoană de încredere cu care elevii ar putea să discute despre incident?	<input type="checkbox"/>	<input type="checkbox"/>	
Personalul, elevii și membrii comunității școlare extinse respectă și aderă la PUA?	<input type="checkbox"/>	<input type="checkbox"/>	
Există riscul ca incidentul să fie repetat de către agresor sau să fie îndreptat împotriva aceleiași victim? Există o nevoie pentru activități de conștientizare sau alte acțiuni?	<input type="checkbox"/>	<input type="checkbox"/>	

8. Listă de verificare: Informații pentru părinți
Facem acest lucru în școala noastră?

Politică

- | | | | |
|---|--------------------------|--------------------------|--------------------------|
| 1. Părinții sunt rugați să-și asume un rol activ eSafety la școală și să întărească mesajele cheie. Acest lucru este subliniat în mod clar în acordul familie/școală. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
|---|--------------------------|--------------------------|--------------------------|

Practică

- | | | | |
|---|--------------------------|--------------------------|--------------------------|
| 2. Sesiunile pentru părinți legate de eSafety au loc cel puțin o dată pe an. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3. Mesajele privind eSafety sunt diseminate către părinți prin intermediul unor medii diferite de comunicare. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 4. Elevii sunt implicați în transmiterea mesajelor eSafety către părinți. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

COMPONENTA POLITICI ESAFETY

1. Listă de verificare: Politica școlară
Facem acest lucru în școala noastră?

	Da	Parțial	Nu
Infrastructură			
1. Politica eSafety a școlii conține informații despre sisteme de securitate și firewall.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. Toți profesorii primesc instruire în mod regulat pe aspecte ce țin de eSafety și înțeleg folosirea ambelor sisteme, atât educațional, cât și administrativ.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. O persoană este responsabilă pentru achiziționarea și actualizarea licențelor software (informatician sau manager de sistem)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4. Politica de eSafety oferă indicații clare cu privire la folosirea adecvată și inadecvată a comunicării online între diferiți actori implicați (elev, profesor, părinte).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Politică			
5. O singură persoană este responsabilă ca toate aspectele incluse în politica eSafety să fie discutate cu toți actorii implicați (Coordonatorul eSafety).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6. Politica eSafety a școlii acoperă următoarele aspecte: folosirea imaginilor și clipurilor digitale, protecția datelor, activități nepotrivite și drepturi de autor, utilizarea dispozitivelor mobile și imagini ilegale.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Practici			
7. O procedură de gestionare a incidentelor clară și ușor de accesat este implementată.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8. Pregătirea personalului în domeniul eSafety este făcută cel puțin anual.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9. Toți profesorii primesc instruire în mod regulat pe teme ce țin de eSafety și sunt implicați în formare profesională continuă.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10. Politica eSafety a școlii face referire la integrarea eSafety in curriculum.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2. Listă de verificare: Politică de Utilizare Acceptabilă (PUA)

Facem acest lucru în școala noastră?

	Da	Parțial	Nu
Infrastructură			
1. Infrastructura școlară poate fi adaptată unor noi inițiative precum aducerea dispozitivelor personale, iar PUA este modificată în consecință.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Politică			
2. Școala are o PUA care este actualizată constant.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. Atunci când este revizuită PUA, sunt implicați toți actorii.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Practică			
4. Personalul vorbește elevilor despre PUA pentru a se asigura că există o înțelegere comună	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5. Personalul, elevii și membrii comunității școlare extinse respectă prevederile și aderă la PUA.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

3. Listă de verificare: Parole sigure

Facem acest lucru în școala noastră?

	Da	Parțial	Nu
Infrastructură			
1. Infrastructura noastră de ITC este securizată; cere utilizatorilor în mod regulat să își reînnoiască parola pentru a accesa sistemul.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Politică			
2. PUA conține informații despre parole.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. Profesorii discută în mod periodic cu elevii despre importanța unor parole eficiente și sigure.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Practică			
4. Protecția datelor este discutată ca parte a curriculumului.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

4. Listă de verificare: Realizarea și publicarea de imagini și clipuri video la școală

Facem acest lucru în școala noastră?

	Da	Parțial	Nu
Infrastructură			
1. Un membru al personalului este responsabil pentru verificarea că lângă pozele elevilor de pe website nu apar date personale.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Politică			
2. Există o politică clară în ceea ce privește imaginile și fotografiile. Toți profesorii, părinții, elevii și membrii comunității școlare sunt informați în mod regulat cu privire la această politică.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Practici			
3. Școala păstrează o bază de date unde politica și documentele suport (accord de fotografiere/filmare) pot fi găsite cu ușurință.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4. Toți profesorii știu la cine pot apela pentru îndrumare în cazul în care au nelămuriri.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5. Toată comunitatea școlară, inclusive elevii, au primit instruire cu privire la producerea de fotografii și utilizarea rețelelor sociale.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6. Un memento este trimis tuturor înainte de un eveniment școlar.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

5. Listă de verificare: Școlile pe rețelele sociale

Facem acest lucru în școala noastră?

	Da	Parțial	Nu
Politică			
1. Personalul școlii este informat despre politicile care țin de utilizarea rețelelor sociale și posibilele restricții.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. Elevii au fost informați despre politica școlii cu privire la folosirea rețelelor sociale, precum și modele de bune practică, folosirea în siguranță a rețelelor sociale și posibile restricții.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Practică			
3. Atelierele destinate personalului despre utilizarea rețelelor sociale sunt ținute cel puțin la fiecare șase luni.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4. Părinții sunt informați și implicați în politicile care țin de utilizarea rețelelor sociale.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5. Elevii sunt implicați în folosirea rețelelor sociale la școală. Elevii au rolul de mentori pentru alți elevi.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

COMPONENTA INFRASTRUCTURĂ

1. Listă de verificare: Protejarea datelor sensibile în școală

Facem acest lucru în școala noastră?

	Da	Parțial	Nu
Infrastructură			
1. Există sisteme informatice separate pentru administrație și învățare.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. Protecția antivirus este actualizată constant.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. În vederea stocării și encriptării datelor, sprijin profesional este cerut.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Politică			
4. Avem un protocol riguros aplicat atunci când vine vorba despre descărcarea/trimiterea/printarea datelor sensibile.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5. Informații despre parole sunt incluse în PUA.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6. Avem o relație bună cu persoana de contact din cadrul Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal. ²	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Practică			
7. Organizăm sesiuni de formare pentru angajații noștri susținute de o persoană specializată.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8. Organizăm anual cel puțin o întâlnire cu membrii personalului pentru a discuta despre importanța protecției datelor cu caracter personal, inclusiv riscurile care țin de inginerie socială ³ .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9. O procedură de gestionare a incidentelor este în vigoare.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2. Listă de verificare: Protejarea dispozitivelor împotriva malware

Facem acest lucru în școala noastră?

	Da	Parțial	Nu
Infrastructură			
1. Pe toate computerele/dispozitivele școlii există protecție antivirus și firewall-uri activate, iar acestea sunt actualizate constant.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. Websiturile nedorite și ferestrele pop-up sunt blocate în mod permanent pe toate dispozitivele din școală.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Politică			
3. PUA conține un protocol strict în ceea ce privește descărcarea de fișiere, verificarea emailului și folosirea dispozitivelor portabile.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Practică			
4. Membrii personalului le sunt furnizate sesiuni de formare de către un expert.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5. Există o persoană dedicată care se ocupă de breșele de securitate care pot apărea.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6. Există o procedură pentru gestionarea incidentelor în vigoare.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

² Puteți găsi detaliile despre persoana de contact din țara dumneavoastră la adresa: http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm.

³ Websiturile de inginerie social se referă la siturile care păcălesc utilizatorul să intre pe un alt website sau să deschidă un atașament care conține malware.

- | | | | |
|---|--------------------------|--------------------------|--------------------------|
| 7. Elevii sunt informați despre cum pot scana fișierele pentru malware, pe dispozitivele școlare. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 8. Elevii sunt informați despre importanța blocării anumitor conținuturi pe computerele școlii. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

3.Listă de verificare: Folosirea dispozitivelor de stocare externe
Facem acest lucru în școala noastră?

	Da	Parțial	Nu
Infrastructură			
1. Protecția antivirus protection este instalată și actualizată constant.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Politică			
2. Reguli care țin de folosirea dispozitivelor de stocare externe sunt incluse în PUA.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. Personalul nu salvează date sensibile pe dispozitive de stocare externe.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4. Proceduri de gestionare a incidentelor au fost implementate, în special în cazurile în care s-a pierdut un dispozitiv extern de stocare care conține date sensibile despre elevi.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Practică			
5. Personalului și elevilor li se cere să scaneze pentru viruși orice dispozitiv de stocare extern atunci când îl folosesc pe un computer al școlii.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6. Personalul și elevii sunt informați/instruiți cum să scaneze pentru viruși un dispozitiv.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7. Personalul și elevii sunt informați cu privire la procedura de gestionare a incidentelor și o respect pe aceasta. (ex. dispozitiv pierdut, infecție cu malware)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

4. Listă de verificare: Utilizarea telefoanelor mobile în școală
Facem acest lucru în școala noastră?

	Da	Parțial	Nu
Infrastructură			
1. Rețeaua noastră Wi-Fi nu este accesibilă telefoanelor mobile.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. Rețeaua noastră Wi-Fi poate fi accesată de către elevi, dar este diferită de rețeaua securizată, destinată personalului.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Politică			
3. PUA conține un protocol strict referitor la utilizarea dispozitivelor mobile în școli.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4. Politica școlară conține instrucțiuni clare referitoare la posesia și utilizarea dispozitivelor mobile în școală și consecințele încălcării unei astfel de politici.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Practică			
5. Utilizarea dispozitivelor mobile este încorporată într-un mod constructiv în curriculum.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6. Profesorii, elevii și părinții sunt bine informați despre politica de folosire a dispozitivelor mobile la școală.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7. O procedură strictă este aplicată de către personal pentru a gestiona încălcările politicii care ține de dispozitivele mobile și confiscarea acestora.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

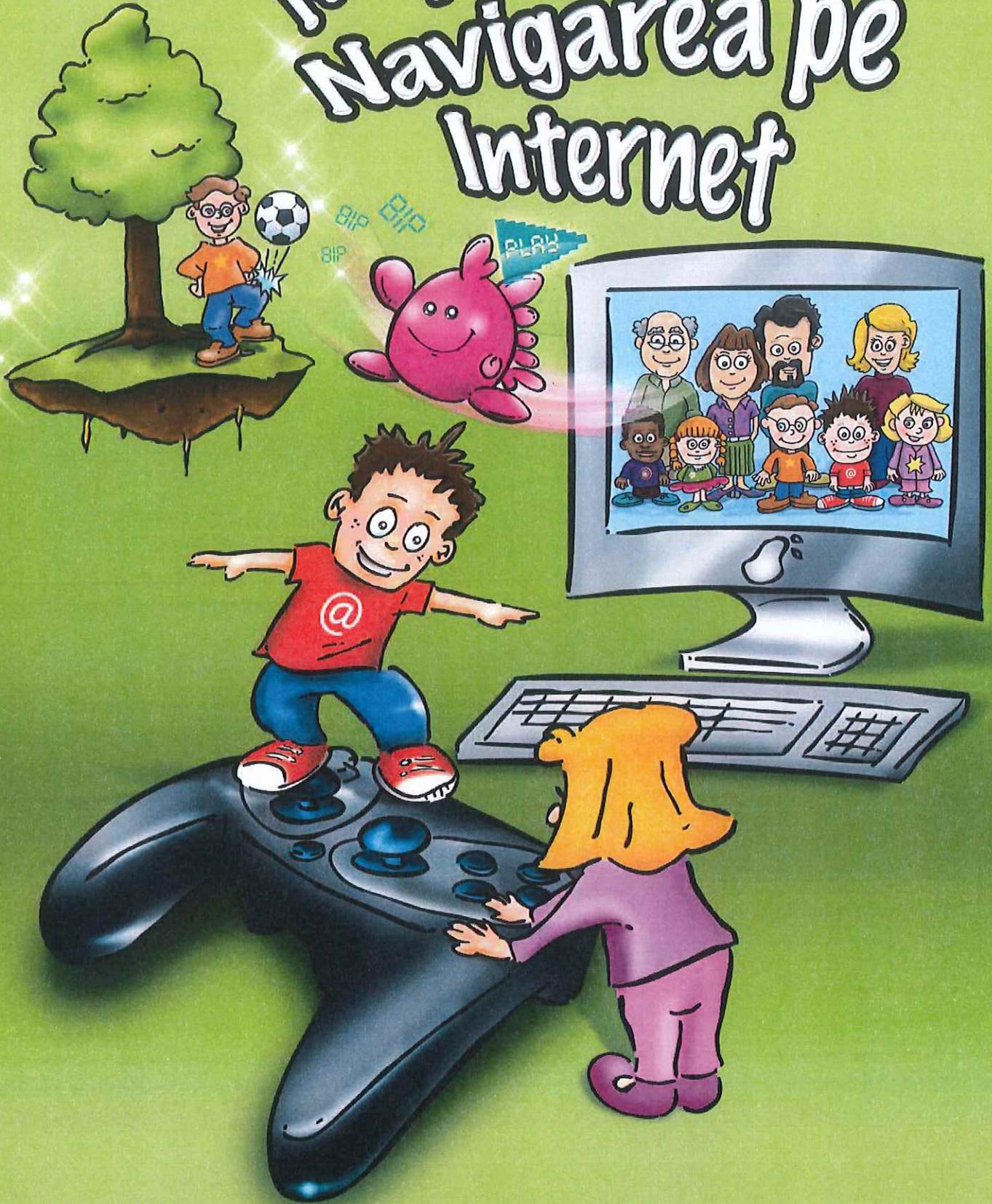
Ai întrebări sau ai nevoie de consiliere din partea specialiștilor în siguranță online?

**Scrive un mesaj echipei Ora de Net la adresa ajutor@oradenet.ro
sau pe pagina de Facebook - <https://www.facebook.com/SigurPeNet>.**

Suntem aici să te susținem pe tine și colegii tăi!



Ne jucăm și învățăm: Navigarea pe Internet



Cu sprijinul:



ins@fe

@sigur.info



upc

Despre această broșură

Astăzi, copiii accesează Internetul de la o vârstă tot mai fragedă. Ca atare, această broșură își propune să introducă conceptele aferente tehnologiilor moderne în vocabularul și activitățile lor cotidiene.

Broșura le oferă copiilor cu vârste cuprinse între 4 și 8 ani peste 30 de pagini cu jocuri și activități recreative, însă contribuie și la consolidarea competențelor lor lingvistice, matematice, sociale și culturale. De asemenea, le permite să-și facă o idee despre impactul pe care-l pot avea tehnologiile moderne asupra vieții lor cotidiene. Mai presus însă de aceste aspecte, oferă părinților și cadrelor didactice ocazia de a discuta aceste subiecte importante cu copiii.

Deși materialul a fost conceput astfel încât copiii să-l poată parcurge singuri, multe dintre exerciții au un nivel mai profund. Broșura caută să stimuleze discuțiile dintre părinți și cadre didactice, pe de o parte, și copii și elevi, pe de altă parte, pe marginea unor subiecte precum protecția datelor cu caracter personal și tehnologiile moderne, dat fiind că aceste subiecte joacă deja un rol important în viața acestora.

Tabelul de la pagina 4 conține un sinopsis al temelor prezentate în broșură și al exercițiilor aferente. Pentru informații suplimentare, vizitați www.saferinternet.org. Vă recomandăm să consultați cuprinsul, pentru că acolo veți găsi informații mai ample despre obiectivele pedagogice ale fiecărui joc și despre mesajele pe care dorim să le transmitem copiilor.

Despre Insafe

Rețeaua Insafe a fost înființată în 2004 și are rolul de sensibilizare a opiniei publice, fiind vârf de lance al programului „Un Internet mai sigur” al Comisiei Europene.

În prezent, Insafe cuprinde un centru de informare, o linie telefonică de asistență, consilii ale tinerilor în 30 de țări din Europa și din afara ei, precum și un consiliu paneuropean, care se reunește o dată pe an. Pentru informații suplimentare, vizitați www.saferinternet.org.

Programul „Un Internet mai sigur” al Comisiei Europene a fost inițiat în 1999 și își propune să protejeze tinerii în mediul online și să promoveze utilizarea responsabilă și sigură a tehnologiilor de navigare pe Internet.

Programul cuprinde următoarele direcții de acțiune:

- sensibilizarea opiniei publice
- lupta împotriva conținutului online dăunător și ilegal
- asigurarea unui mediu online mai sigur
- crearea unei baze de date despre siguranța online.

Pentru informații suplimentare, vizitați <http://ec.europa.eu/saferinternet>.

Caiet de lucru
Bine ai venit!

Hai să ne distrăm împreună!

Acest caiet îi aparține:

prenume:

nume:

Sumar „Ne jucăm și învățăm: Navigarea pe Internet”

Fiecare pagină a broșurii este notată cu unul, două sau trei simboluri ★ în funcție de nivelul de dificultate și de necesitățile elevilor de 4-8 ani.

★ = ușor/ vârsta 4-5 ani ★★ = moderat/ 6-7 ani ★★★ = dificil/ peste 8 ani

Temă	Pagina	Aspecte TIC	Exerciții:	Competențe/obiective
Înapoi la școală	p.6*, p.7	Dispozitive TIC deținute	Găsește perechea, descoperă diferențele.	Să compare și să descopere deosebirile. Simboluri ale statutului social și agresiunea.
Familie și prieteni	p.8, p.9*	Profiluri și intimitatea online	Descoperă corespondențe între profiluri, creare profil propriu.	Datele din profilul meu: să perceapă diferența dintre public și privat, să gândească critic cu privire la informațiile furnizate.
Stil de viață sănătos	p.10*, p.11*	Atingerea unui echilibru în activitățile cotidiene	Intervale orare și lipire abțibilduri, povestire	Să reflecteze asupra activităților, să le ordoneze, să stimuleze gândirea critică asupra timpului rezervat învățării, jocului, discuțiilor, igienei etc.
Acțiuni și funcții	p.12, p.13	Dispozitive multifuncționale, convergență	Descoperă corespondențe între dispozitive și calități și capacități.	Să înțeleagă că unele dispozitive pot să realizeze aceeași acțiune, iar un dispozitiv poate să realizeze mai multe acțiuni.
Ce-mi poți spune despre...?	p.14, p.15	Manipularea datelor	Analiză: cum s-a întâmplat.	Să încurajeze gândirea critică, să facă distincția între real și virtual.
Transfer de informații	p.16*, p.17	Protejarea datelor cu caracter personal	Divulgare date și păstrarea confidențialității	Să facă diferența dintre tangibil și intangibil, real și virtual. Gândire critică despre protejarea informațiilor și/sau obiectelor
Învățare	p.18	Competențe online și offline	Cuantificare și identificare competențe și capacități	Cunoașterea de sine, metacunoaștere (să reflecteze la acțiunile proprii).
Tehnologia actuală	p.19*	Evoluția tehnologiei	Ce foloseau părinții și bunicii mei?	Să vorbească despre trecut și viitor, despre evoluția tehnologiei.
Valori	p.20*	Costurile tehnologiei	Ordonare și numărare, descoperirea valorilor	Valoarea dispozitivelor TIC, gândire critică asupra prețului acestor dispozitive, pe care uneori copiii consideră că li se cuvin de la sine.
Limbă	p.21	Simboluri TIC	Descoperă corespondențe între simboluri și țări.	Să conștientizeze diferențele culturale.
Protejarea obiectelor	p.22, p.23, p.28, p.30	Protejarea propriului computer	Să creeze parole, să potrivească obiectele cu cheia lor, jocuri de cuvinte.	Să soluționeze probleme, să descopere noi simboluri, să decodifice mesaje.
Protecția personală	p.24*, p.29*	Funcții de ajutor și servicii bazate pe localizare	Cuvinte încrucișate despre siguranță, labirint	Să-și dezvolte limbajul. Să înțeleagă conceptul de anonim și servicii bazate pe localizare.
Emoții/responsabilitate (acțiune/reacțiune)	p.25, p.26	Comunicare online	Să descopere corespondențe între emoticon-uri și incidente, să reacționeze la mesaje.	Să contracareze hărțuirea online, să învețe să-și exprime/manifeste emoțiile și empatia.
Huliganism	p.27*	Comunicare online și offline	Povestire	Să facă distincție între real și virtual, să ceară ajutor, să discute despre probleme.

*Exerciții cu nivel suplimentar. Părinții și cadrele didactice pot găsi explicații suplimentare pentru activitățile cu elevii la adresa www.saferinternet.org

Să facem cunoștință cu membrii familiei și cu prietenii acestora

Bunicul

Mama

Tata

Helen,
dădaca



Ben
un prieten

Anna

Tom
un prieten

Alex

Sarah
o prietenă



Înapoi la școală

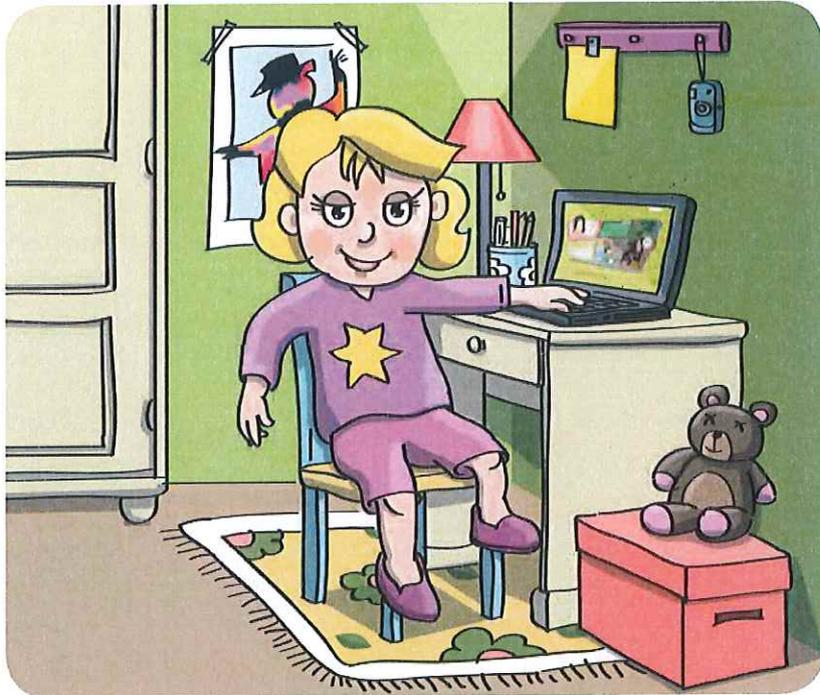
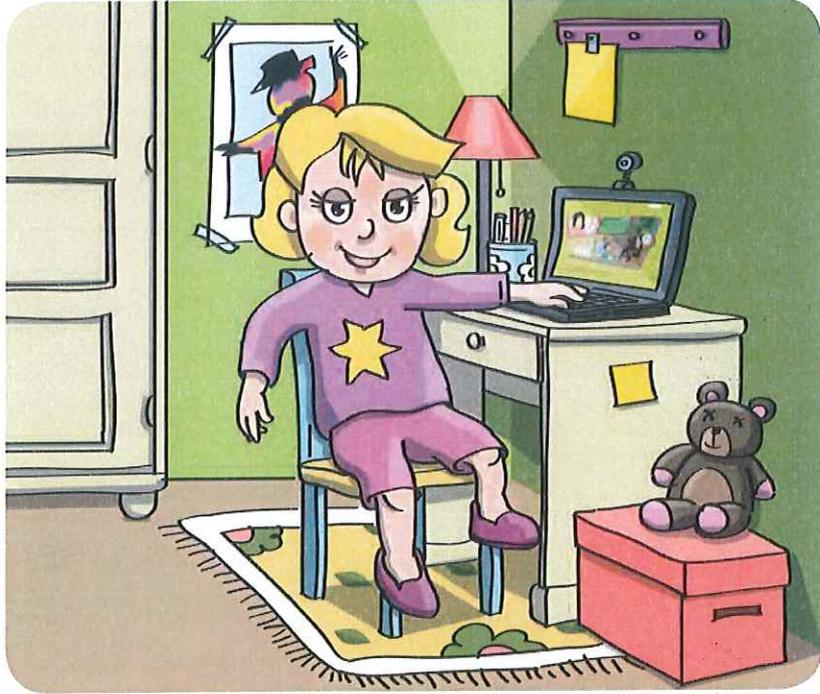
Astăzi, Anna, Tom, Alex și Ben încep școala. Uită-te la ghiozdanele, cutiile pentru mâncare, telefoanele mobile și computerele lor.



Găsește perechile.



Descoperă cele cinci diferențe!





Unește profilul cu persoana potrivită.

1
îmi place să mănânc pizza.
îmi place să cânt la chitară.
Vreau să devin pompier.
îmi place să ascult muzică.

2
îmi place să mă joc pe
computer.
Aș vrea să fiu medic
veterinar.
Locuiesc cu mama și cu
cele două surori ale mele.
îmi plac abțibildurile.

3
îi iubesc pe mama și pe
tata.
îmi place înghețata.
îmi place să merg la plajă.
îmi plac desenele animate.

4
îmi place să joc fotbal.
îmi plac spaghettițele.
Culoarea mea preferată e
albastru.
Am un câine pe nume
Rocco.



Ben



Alex



Sarah



Anna

Eu, familia și prietenii mei!



Pot să le spun totul:



Pot să le spun aproape totul:



Pot să le spun unele lucruri:

Completează-ți profilul!

- Cum te numești? _____
- Câți ani ai? _____
- Unde locuiești? _____
- _____
- Ce număr de telefon ai? _____
- La ce școală înveți? _____
- Care e prietenul tău? _____



Încercuiește imaginile.

Îmi place să mănânc



Îmi place să merg la



Îmi place să



Am un/o

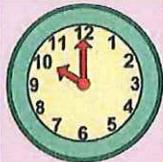


Bifează , ca să vedem cui i-ai spune aceste informații.



O zi din viața mea:

Ce ai făcut astăzi? Pune abțibildurile (A) în intervalul orar corect.



Blank space for drawing activities between 8:00 and 9:00.

Blank space for drawing activities between 9:00 and 10:00.

Blank space for drawing activities between 10:00 and 11:00.

Blank space for drawing activities between 11:00 and 12:00.

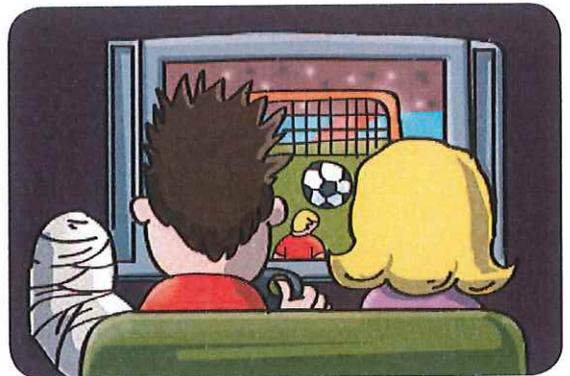
Blank space for drawing activities between 12:00 and 1:00.

Blank space for drawing activities between 1:00 and 2:00.

Alege un moment al zilei.
Desenează ce ai făcut atunci.



Povesteste ce s-a întâmplat.



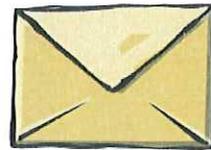


Care obiecte pot...

face o fotografie:



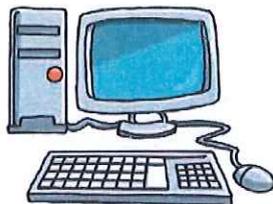
trimite o fotografie:



reda muzică:

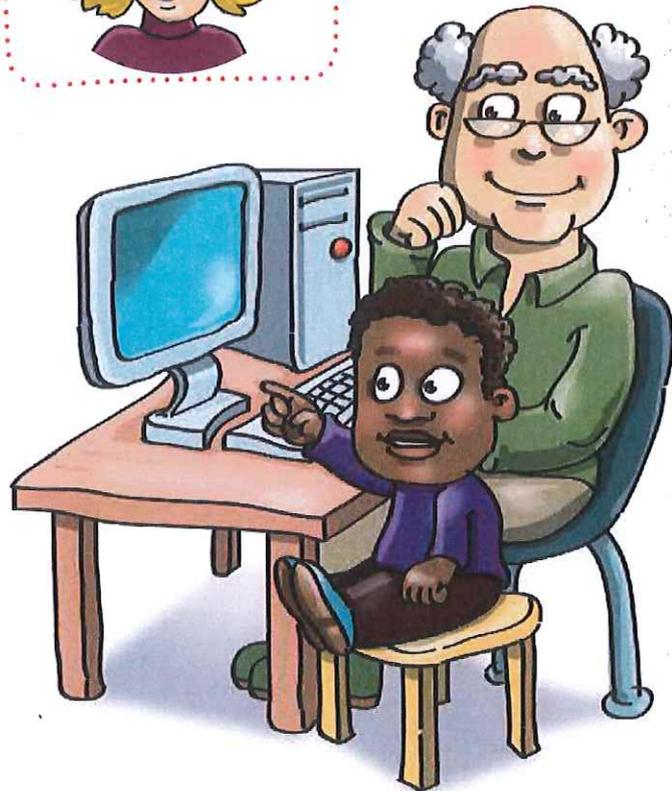
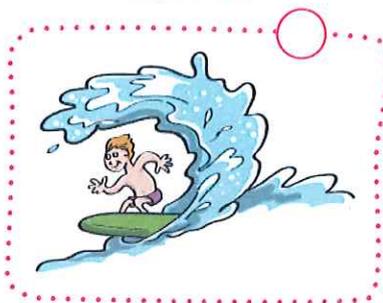
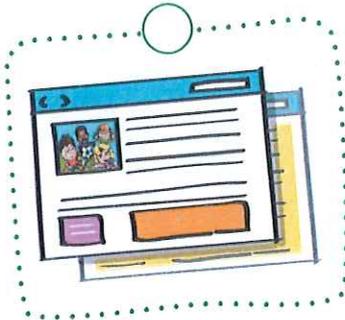


scrie o scrisoare:



Ce poți face pe computer?

Bifează imaginile corecte.





Ce-mi poți despre...? spune

Unește punctele și descoperă ce obții atunci când combini imaginile.

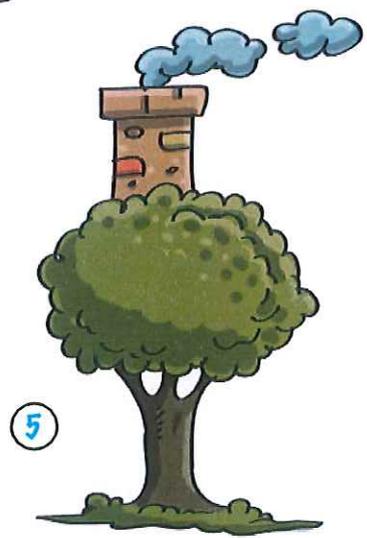
Puzzle 1: A dog and a house. The dog is formed by connecting points 1-39. The house is formed by connecting points 1-39.

Puzzle 2: A boy with glasses and a shark. The boy is formed by connecting points 1-20. The shark is formed by connecting points 1-20.

Puzzle 3: A boy and a UFO. The boy is formed by connecting points 1-19. The UFO is formed by connecting points 1-19.



Încercuiește
imaginile
care nu ți se
par reale!





Pr tejează-ți informațiile personale

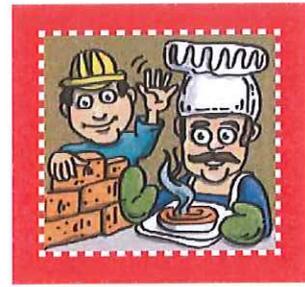
Colorează chenarele și arată cui i-ai încredința următoarele:



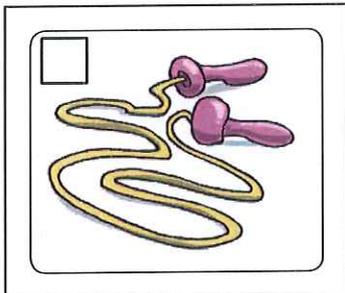
familiei



familiei și prietenilor



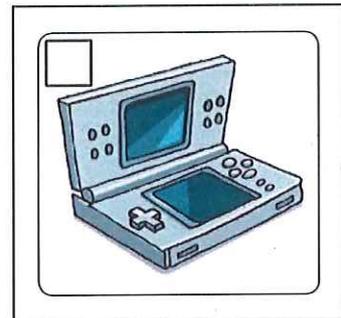
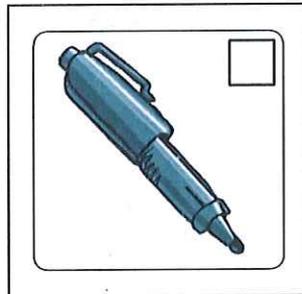
tuturor



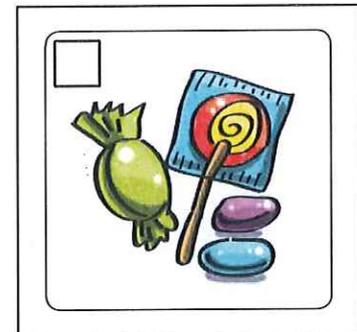
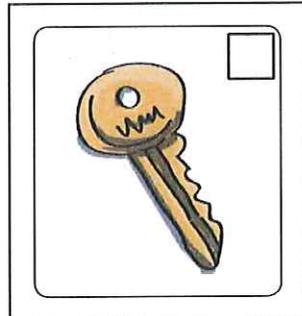
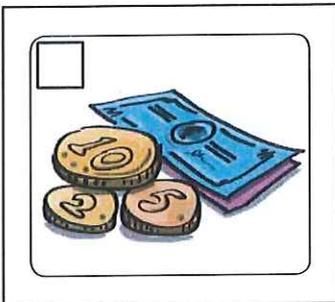
un secret



numele

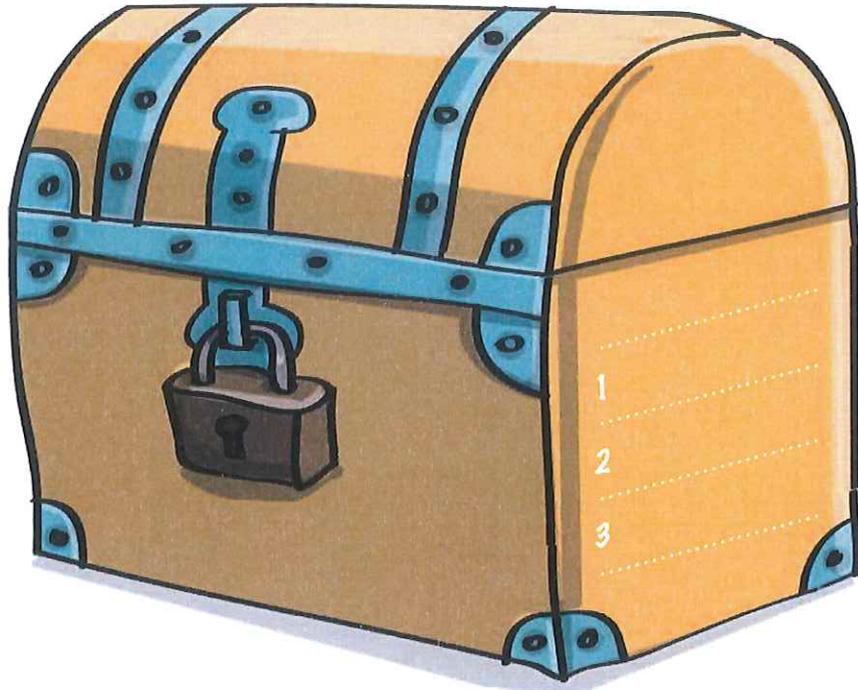


parola

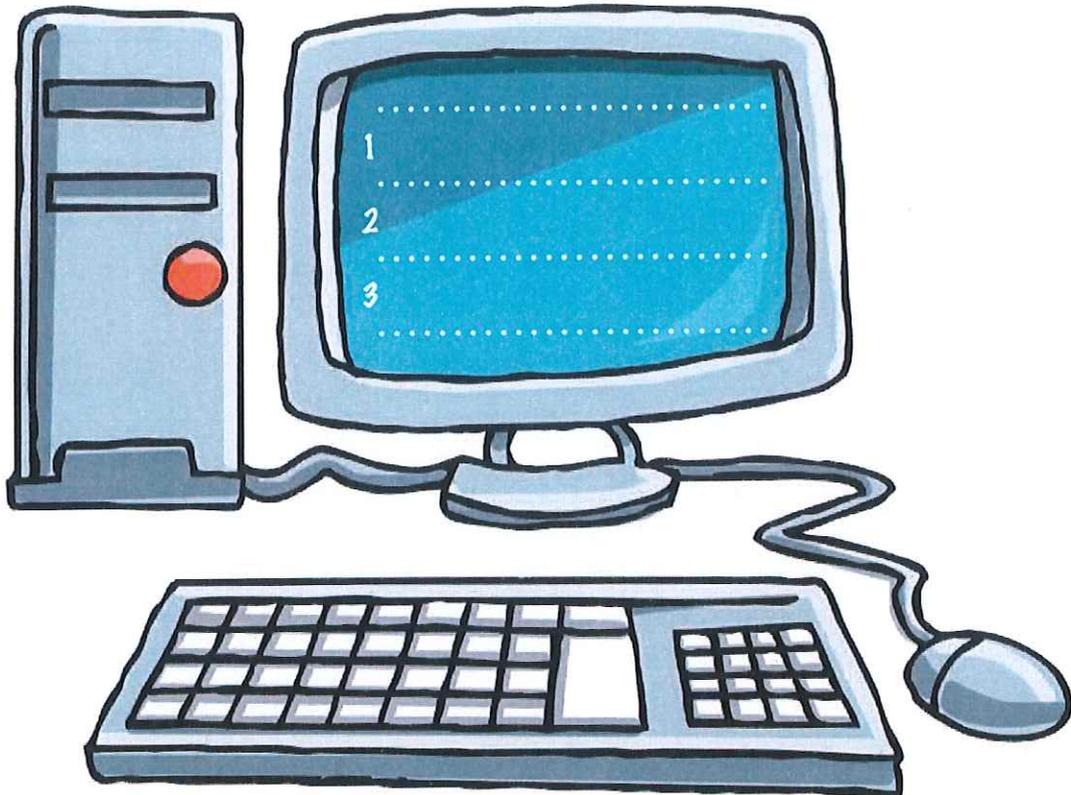


Acum bifează pentru a arăta care obiecte le poți lua înapoi.

Scrie trei lucruri pe care le-ai păstra în siguranță într-un cofăr.



Scrie trei lucruri pe care le-ai păstra în siguranță pe computerul tău.





La ce te pricepi?

Pentru a ne arăta, pune abțibildurile (B) în cele trei secțiuni.

Mă pricep la

Mă pricep destul
de bine la

Nu prea mă pricep la

Bifează cercurile și spune-ne dacă...



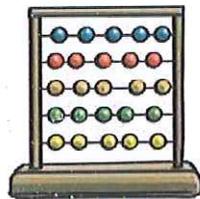
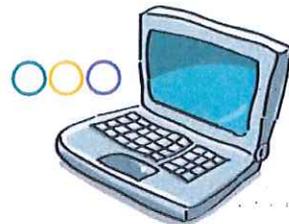
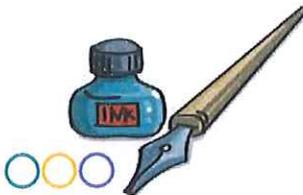
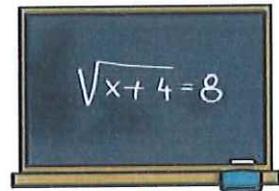
...bunicii tăi le-au folosit



...părinții tăi le-au folosit



...tu le-ai folosit





Un CD este egal cu 1,
un telefon mobil este egal cu 3.
Ce valoare au celelalte obiecte?

Diagram showing the relative values of objects based on the given information:

- A CD is equal to 1 (indicated by a red box around the number 1).
- A USB drive is equal to an empty box.
- A mobile phone is equal to 3 (indicated by a blue box around the number 3).
- A handheld game console is equal to an empty box.
- A computer monitor is equal to an empty box.

Să facem și câteva calcule.

$$\text{USB drive} = \text{CD} + \text{CD} = \square$$

$$\text{Handheld game console} = \text{Mobile phone} + \text{CD} = \square$$

$$\text{Computer monitor} = \text{USB drive} + \text{CD} + \text{Mobile phone} + \text{CD} = \square$$

$$\text{Laptop} = \text{Mobile phone} + \text{USB drive} + \text{Handheld game console} = \square$$



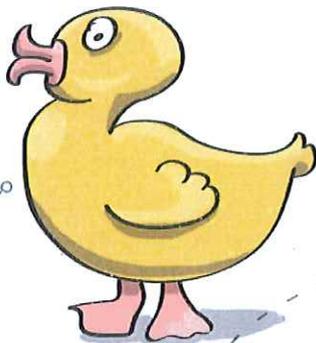
Simbolul



Urmărește liniile și află cum se numește simbolul @ în aceste țări.



Danemarca



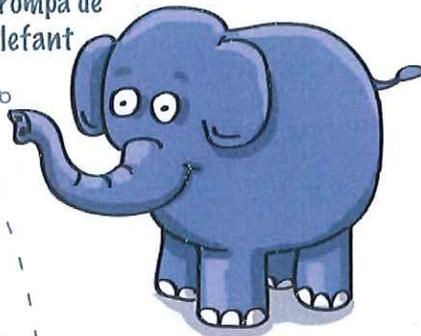
Rățușca

Coadă de maimuță



Norvegia

Trompă de elefant

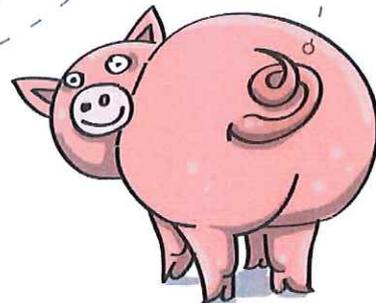


Coreea

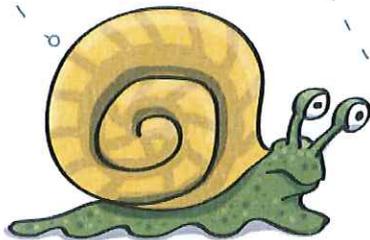


Țările de Jos

Coadă de porc



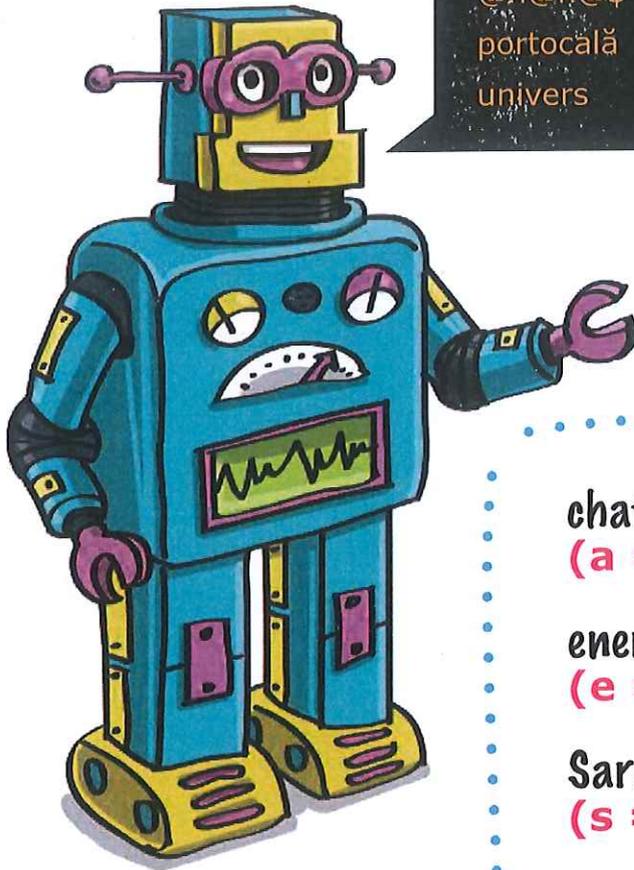
Melcul



Grecia



Ajutați robotul să creeze parole noi.



@n@n@\$ = ananas
portocală = p0rt0c@l@
univers = un!v€rș

chat
(a = @)

energie
(e = €)

Sarah
(s = \$)

leșire
(i = !)

televiziune
(t = +, u = μ)

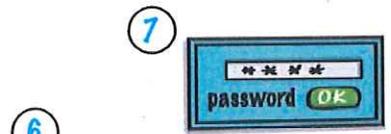
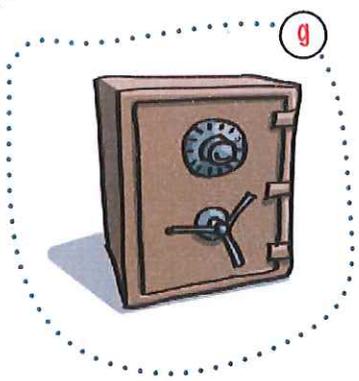
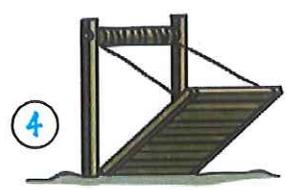
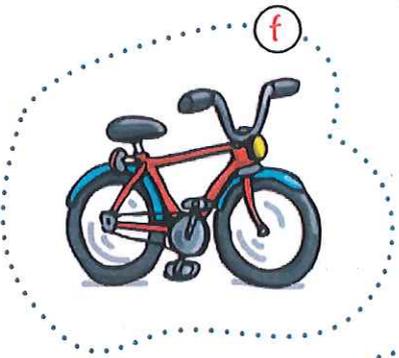
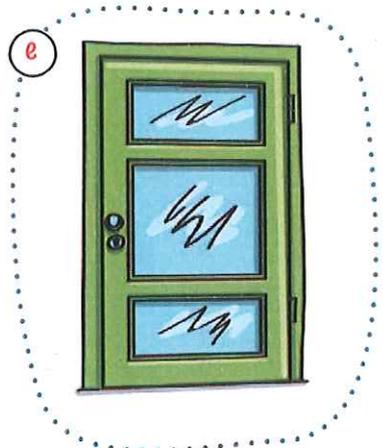
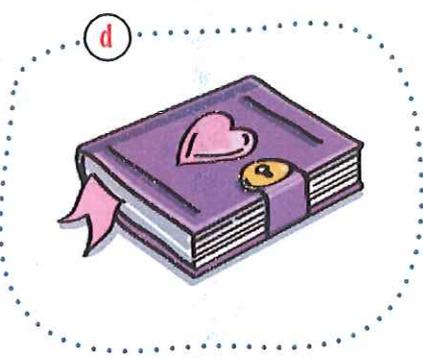
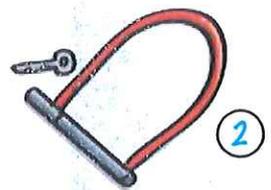
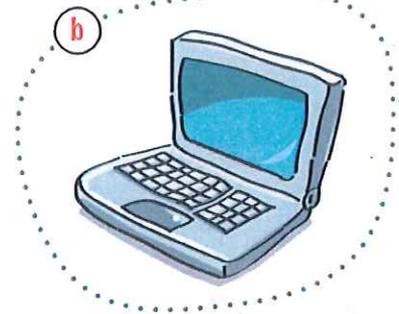
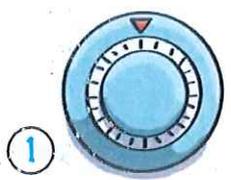
zero
(z = 7, o = 0)

internet
(i = !, e = €)



Sub lacăt!

Unește cheia potrivită cu obiectul pe care-l închide.





C U V I N T E încrucișate

Completați spațiile libere!

Grid layout and icons:

- Top-left: Lightning bolt icon (⚡) with a downward arrow pointing to a horizontal word starting with 'P'.
- Top-center: Person swimming icon (🏊) with a downward arrow pointing to a vertical word starting with 'A'.
- Top-right: First aid kit icon (🩹) with a downward arrow pointing to a vertical word.
- Middle-left: Fire icon (🔥) with a downward arrow pointing to a vertical word starting with 'F'.
- Middle-right: Stop sign icon (🛑) with a leftward arrow pointing to a horizontal word starting with 'P'.
- Bottom-right: Exit sign icon (🚪) with a downward arrow pointing to a horizontal word ending with 'S'.
- Bottom-center: Lifebuoy icon (🛟) with a leftward arrow pointing to a horizontal word ending with 'S'.
- Bottom-left: A pair of glasses icon (👓) with an upward arrow pointing to a horizontal word starting with 'D'.

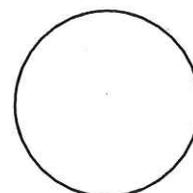
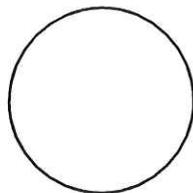
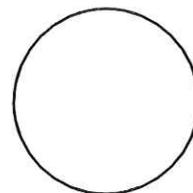
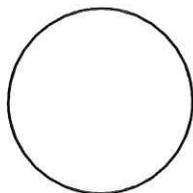
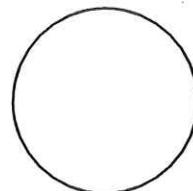
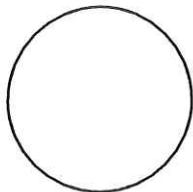
polițist
pericol
ieșire
ajutor
SOS
foc
stop
doctor
prim ajutor

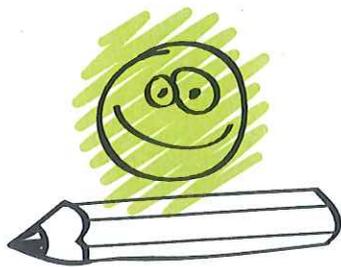


EMOTIC NURI

Cum te simți?

Potrivește abțibildurile cu emoticonuri  cu imaginile corecte.



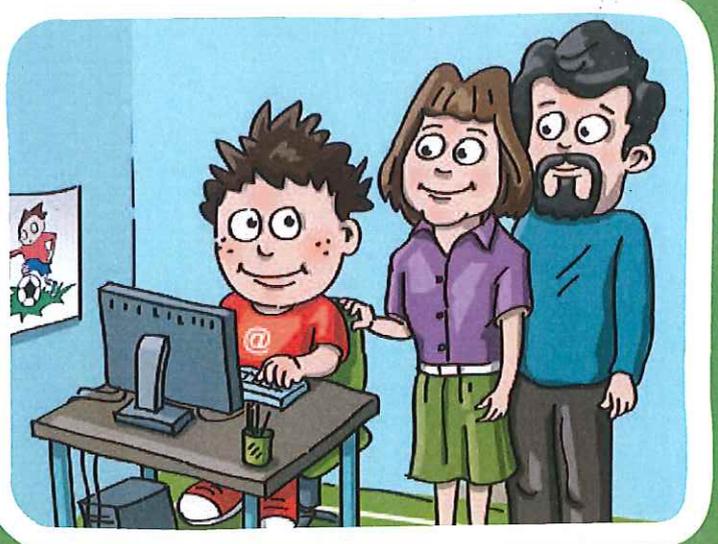
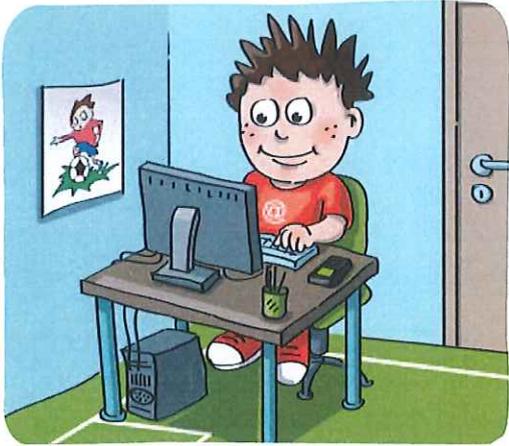


Cum te simți?

Desenează propriile tale simboluri!



Povesteste ce s-a întâmplat.





Tăiați cuvintele 'SPAM' și 'VIRUS' și completați mesajul din
chenar cu literele lipsă.

V	I	R	U	S	B	S	U	V	N
S	A	S	P	A	M	P	V	I	S
P	P	A	R	S	E	A	I	R	P
A	M	A	S	P	A	M	S	U	A
M	A	V	M	A	V	I	A	S	M
I	L	I	A	M	A	P	S	P	M
V	I	R	S	S	P	A	M	N	S
I	M	U	E	P	M	M	S	P	M
R	A	S	A	N	A	E	A	A	A
U	P	J	U	C	P	M	P	P	P
S	S	P	A	M	S	S	A	M	S

Sugestie: căutați cuvintele de la stânga la dreapta, de la dreapta la stânga, în sus, în jos și pe diagonală.

 Alex

.....

B_ _ _ ,

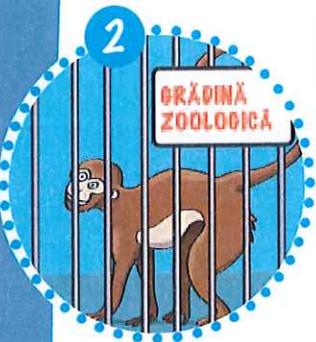
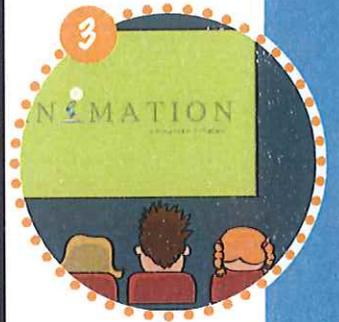
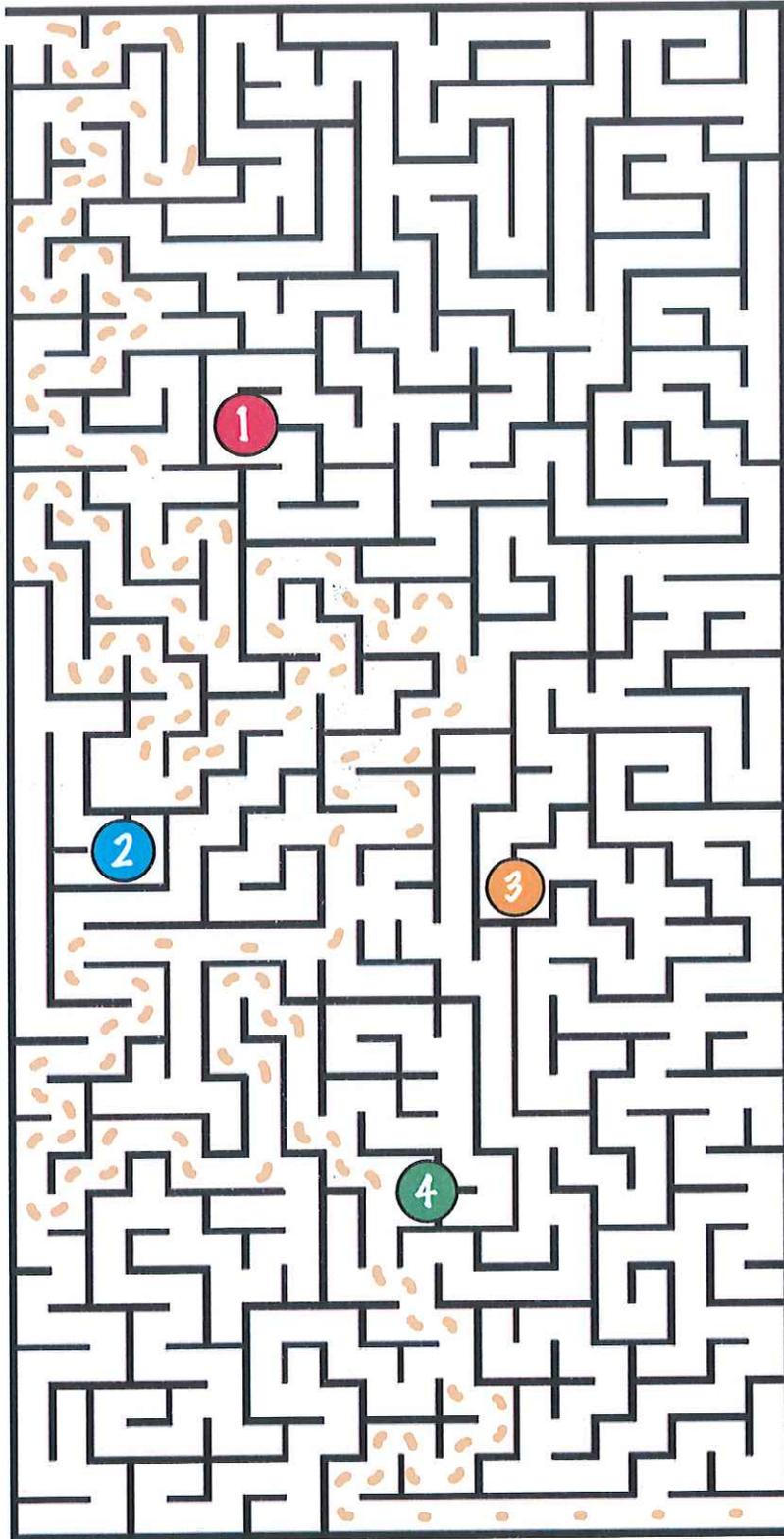
_____ S _____ I _____

_____ M ?

ATENȚIE LA PERICOLE!



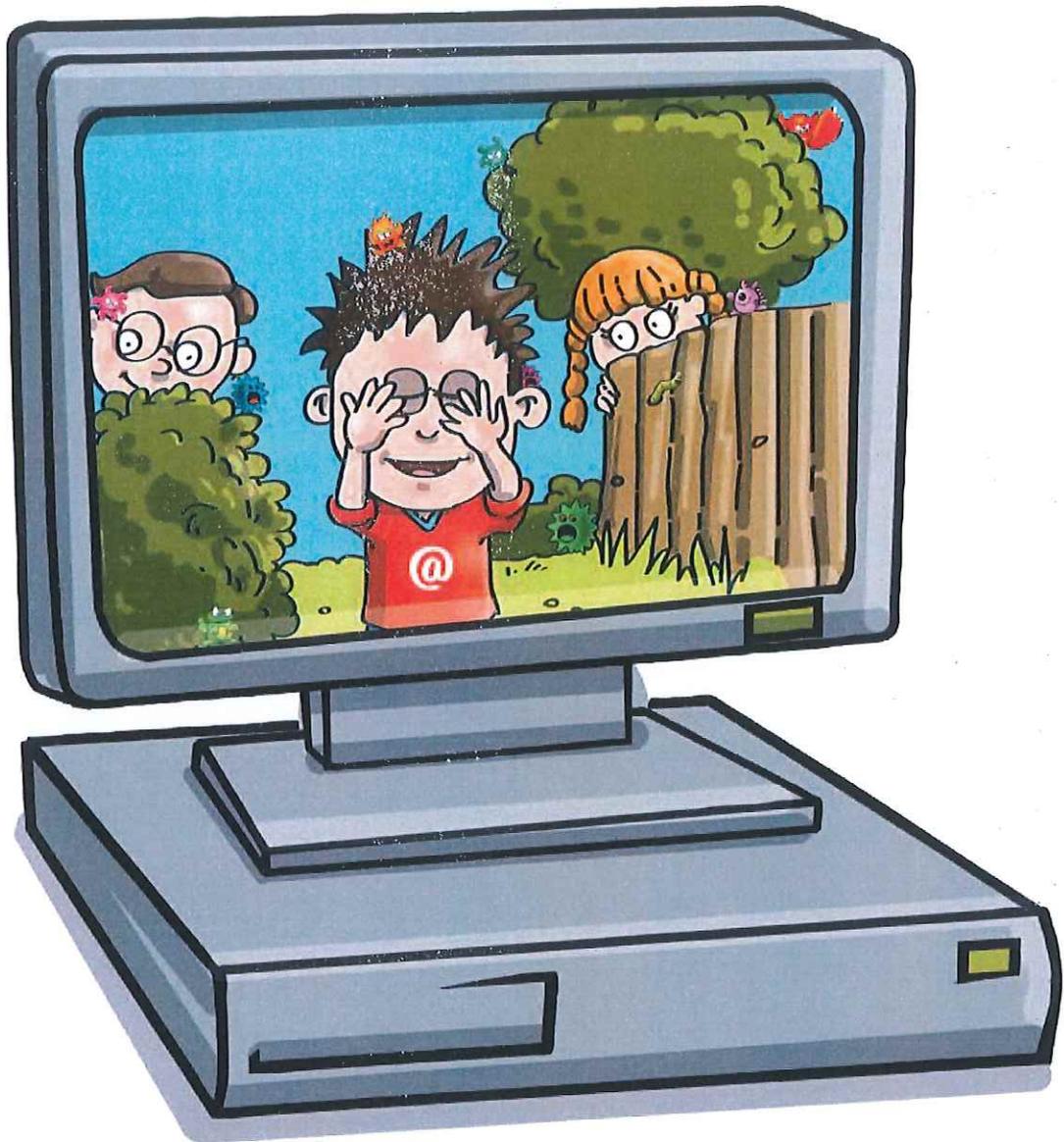
Află unde se duce Anna. Mergi pe urmele ei.





PR TEJEAZĂ-ȚI COMPUTERUL!

Virusii îți invadează computerul. Descoperă-i pe toți zece!



Contactează Centrul Național Insafe

Austria	www.saferinternet.at	Luxemburg	www.bee-secure.lu
Belgia	www.clicksafe.be	Malta	www.mca.org.mt
Bulgaria	www.safenet.bg	Norvegia	www.medietilsynet.no
Cipru	www.cyberethics.info	Polonia	www.saferinternet.pl
Danemarca	www.medieraadet.dk	Portugalia	www.internetsegura.pt
Estonia	www.targaltinternetis.ee	Regatul Unit	www.saferinternet.org.uk
Finlanda	www.ficora.fi	Republica Cehă	www.saferinternet.cz
Franța	www.internetsanscrainte.fr	România	www.sigur.info
Germania	www.klicksafe.de	Rusia	www.saferunet.ru
Grecia	www.saferinternet.gr	Slovacia	www.zodpovedne.sk
Irlanda	www.webwise.ie	Slovenia	www.safe.si
Islanda	www.saft.is	Spania	www.protegeles.com
Italia	www.easy4.it	Suedia	www.medieradet.se
Letonia	www.drossinternets.lv	Țările de Jos	www.mijndigitalewereld.nl
Lituania	www.draugiskasinternetas.lt	Ungaria	www.saferinternet.hu

PEGI

PEGI, cu sprijinul programului „Un Internet mai sigur” al Comisiei Europene, informează părinții despre grupa de vârstă cărora li se adresează jocurile video, cu ajutorul unui set de pictograme care oferă și informații despre conținut. Sistemul este disponibil în 30 de țări europene. Pentru mai multe informații, vizitați www.pegi.info



AUTORI

Creatie

o publicație a European Schoolnet

Insafe (Reteaua europeana cofinantata de Programul Uniunii Europene Safer Internet), cu sprijinul Liberty Global/UPC Romania

Creat in 2011

Imagini si design

Jacqueline M. Jomain
Iddi Fix

Multumiri speciale

Salvati Copiii Romania, Anna Karidi Pirounaki, Marianne Kant-Schaps si profesorilor, parintilor si elevilor care au contribuit la testarea si conceperea acestei publicatii.

COPYRIGHT

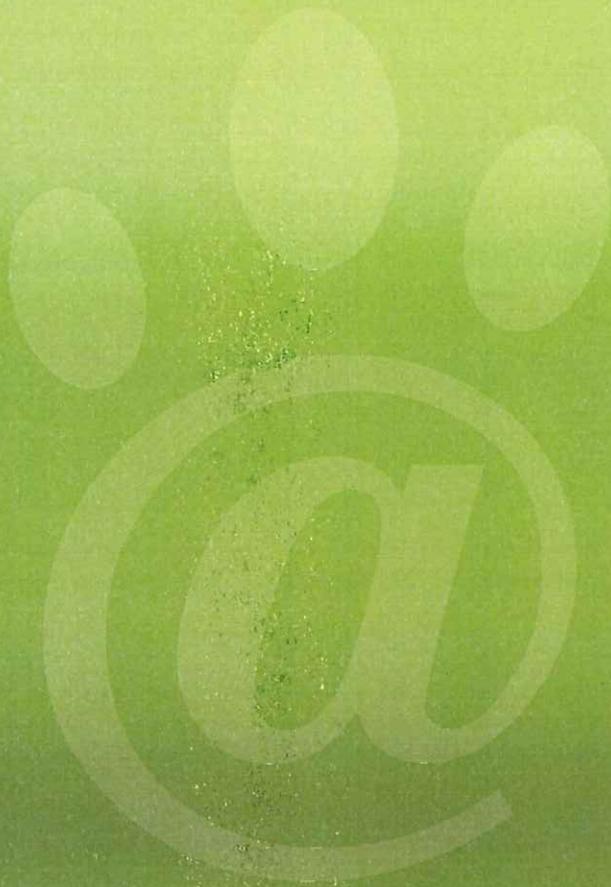
Titlu: Ne jucăm și învățăm: Navigarea pe Internet

Prefix: 9789490477

ISBN-NUMBER: 9789490477448

EAN : 9789490477448

Copyright: această lucrare este produsă sub licența Creative Commons Paternitate-Utilizare Non-Comercială – Fără Modificare 3.0 Unported. Pentru a vedea o copie a licenței, vizitați: <http://creativecommons.org/licenses/by-nc-nd/3.0>



Cu sprijinul:

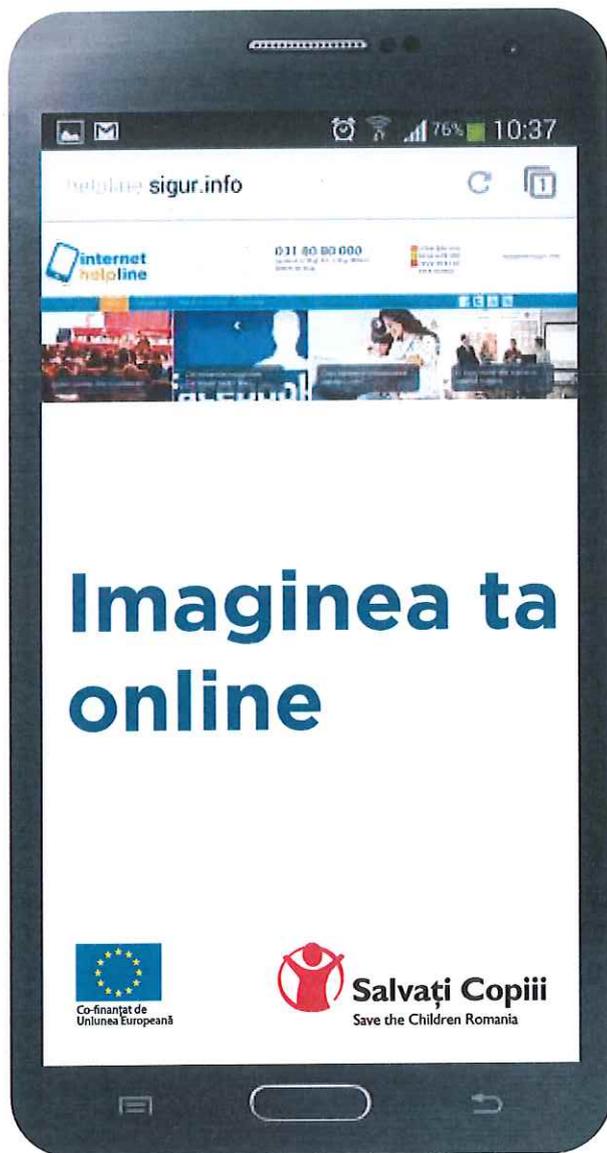


ins@fe

@sigur.info



upc



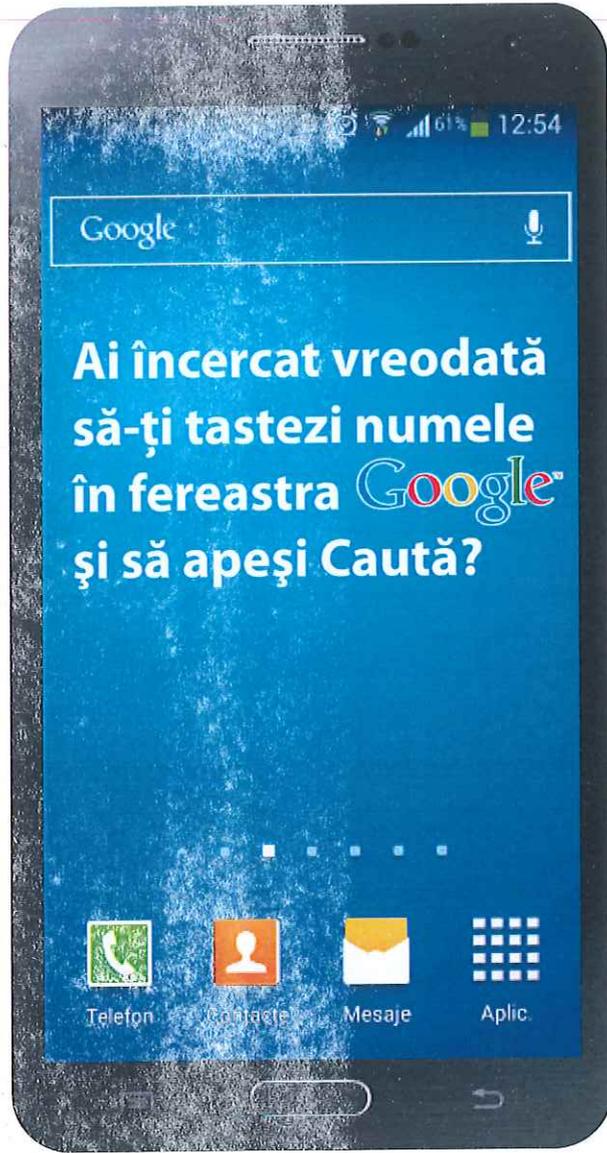
Imaginea ta online



Co-finanțat de
Uniunea Europeană



Salvați Copiii
Save the Children Romania



Google



Ai încercat vreodată
să-ți tastezi numele
în fereastra **Google**
și să apeși **Caută**?



Telefon



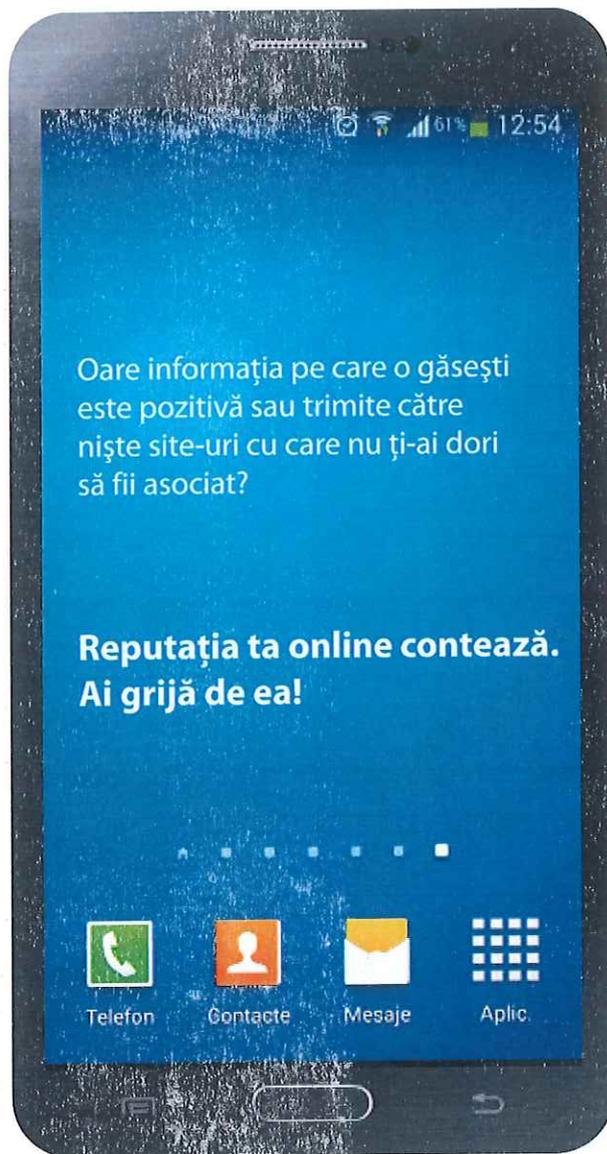
Contacte



Mesaje



Aplic.



Oare informația pe care o găsești
este pozitivă sau trimite către
niște site-uri cu care nu ți-ai dori
să fii asociat?

**Reputația ta online contează.
Ai grijă de ea!**



Telefon



Contacte



Mesaje



Aplic.





10:36 77%



Status Photo Check In



Cum te văd ceilalți pe Internet

13 minutes ago

Postările tale, pozele postate sau în care apari, comentariile, grupurile din care faci parte, numărul de prieteni, aplicațiile pe care le accesezi, paginile favorite sunt câteva dintre elementele care conturează imaginea ta pe rețelele de socializare. Toate acestea te definesc... [Read More](#)

Like Comment Share



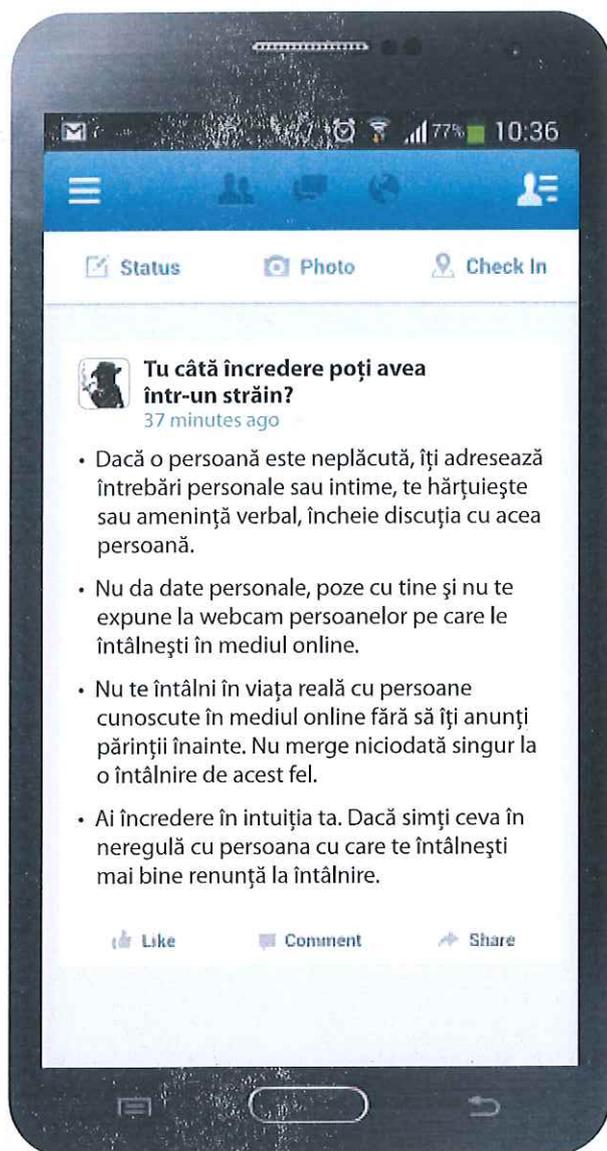
Calitatea contează mai mult decât cantitatea

15 minutes ago

Fii selectiv în legătură cu persoanele pe care le adaugi ca prieteni. Ține minte că atunci când adaugi pe cineva ca prieten el îți poate vedea toate datele personale... [Read More](#)

Like Comment Share





10:36 77%

Status Photo Check In



Tu câtă încredere poți avea într-un străin?

37 minutes ago

- Dacă o persoană este neplăcută, îți adresează întrebări personale sau intime, te hărțuiește sau amenință verbal, încheie discuția cu acea persoană.
- Nu da date personale, poze cu tine și nu te expune la webcam persoanelor pe care le întâlnești în mediul online.
- Nu te întâlnești în viața reală cu persoane cunoscute în mediul online fără să îți anunți părinții înainte. Nu merge niciodată singur la o întâlnire de acest fel.
- Ai încredere în intuiția ta. Dacă simți ceva în neregulă cu persoana cu care te întâlnești mai bine renunță la întâlnire.

Like

Comment

Share





10:36 77%



Status Photo Check In



Setează-ți o parolă puternică și n-o spune nimănui.

Acceptă doar cererile de prietenie din partea persoanelor cunoscute.

Nu posta nimic din ceea ce n-ai vrea ca părinții, profesorii sau angajatorii tăi să vadă.

Fii autentic! Felul tău real de a fi e mai bun decât orice te-ai putea preface a fi.

Ai grijă ce aplicații folosești prin intermediul Facebook, ele pot fi înșelătoare sau viruși.

Like Comment Share



75% 10:40

<https://m.facebook.com/messages>



Dan_14

Sunt hărțuit pe Facebook. Eu am făcut un comentariu politic la o poză și acum persoana respectivă mă înjură și își bate joc de mine prin mesaje și comentarii.

Mă simt foarte rău și vreau să înceteze.

20 noiembrie • Trimis de pe Chat



Violeta_15

Mi-am făcut cont pe Facebook deoarece multe prietene aveau deja și într-o zi un necunoscut din străinătate a intrat într-o discuție cu mine.

La început, totul era frumos, distractiv, ne înțelegeam foarte bine, am crezut că putem fi chiar prieteni până când acesta a început să-mi facă propuneri indecente.

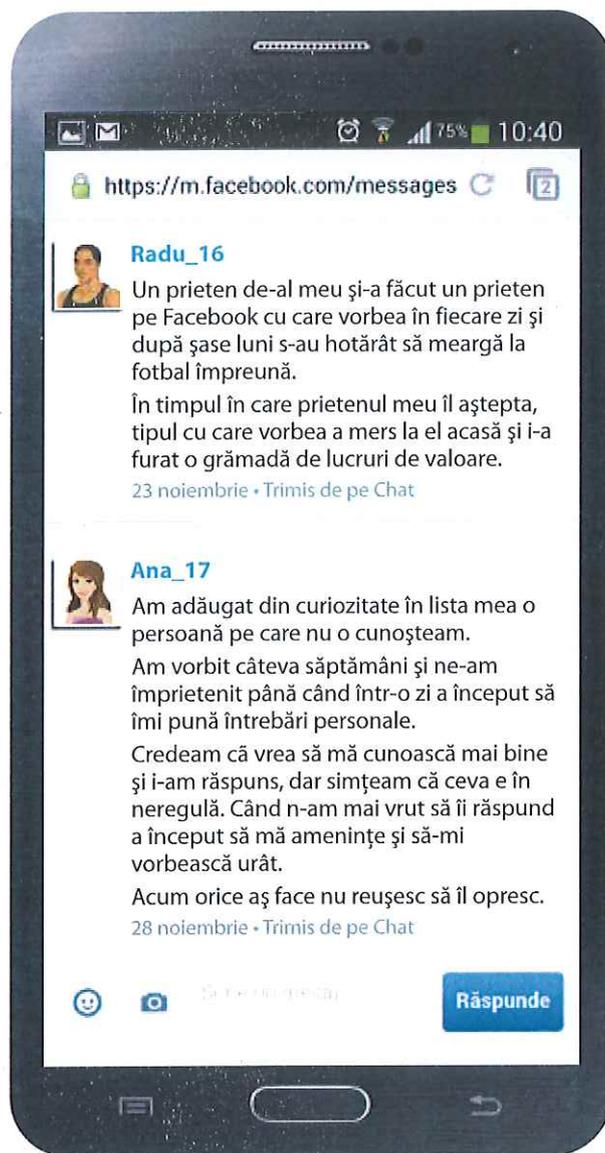
I-am spus că nu putem fi decât prieteni virtuali și a început să îmi adreseze cuvinte jignitoare și să posteze informații nepotrivite pe peretele meu, iar acum toți prietenii mei le pot vedea.

22 noiembrie • Trimis de pe Chat



Scrăiește un mesaj

Răspunde





Co-finanțat de
Uniunea Europeană



Salvați Copiii

Save the Children Romania



Cere un sfat la Helpline

helpline@sigur.info

031 80 80 000

facebook.com/sigurpenet

Kit de acțiune pentru adolescenți



Spune-ți părerea

despre drepturile tale online!

Kit de acțiune pentru adolescenți

Spune-ți părerea despre drepturile tale online!

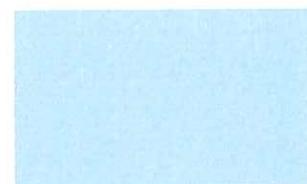
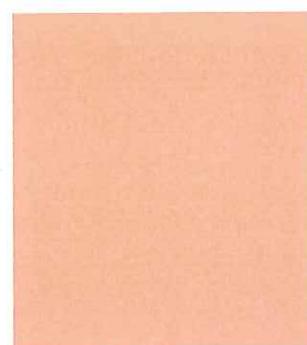
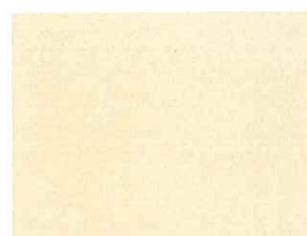
Alătură-te și tu altor tineri europeni pentru ca împreună să creați un ghid online cu privire la drepturile voastre pe Internet. Încarcă creațiile tale* folosind unul dintre cele patru hashtag-uri:

#ParereaTaGDPR, #RomaniaGDPR, #DrepturileCopilului si #OraDeNet.

*Nu uitați să setați opțiunea "Vizibil pentru public/oricine" pentru postările cu care doriți să contribuiți la inițiativa GDPR pentru ca ele să poată fi identificate. Dacă aveți nevoie de informații suplimentare, scrieți-ne la ajutor@oradenet.ro

Cuprins

	Kit de acțiune pentru adolescenți.....	7
1	1. Susține-ți drepturile.....	9
	Activitatea 1 Cunoașterea drepturilor tale!.....	9
	Activitatea 2 Creează un meme cu drepturile tale.....	9
	Activitatea 3 Exerciți-ți drepturile online	9
2	2. Provocări iminente	11
	Activitatea 1 Spune-ți părerea!	11
	Activitatea 2 Găsește un echilibru.....	11
	Activitatea 3 Ascunde sau șterge?	11
	Activitatea 4 Te simți neajutorat?	11
3	3. Cu un pas în viitor	13
	Activitatea 1 Lasă-te cuprins de o lume captivantă.....	13
	Activitatea 2 Fii un pilot inteligent!	13
	Activitatea 3 Selfie din mers.....	13
	Activitatea 4 Jucării Smart?	14
	Activitatea 5 VIDEO-net.....	15
	Activitatea 6 Turnul Babel pe Internet	15
4	4. E timpul de acțiune!.....	17
	Activitatea 1 Planifică o campanie.....	17
	Activitatea 2 Vino cu soluții.....	17
	Activitatea 3 Acționează la nivel local	18
	Activități de reflecție de la egal la egal - pentru profesori și lideri ai tinerilor	19
	Glosar de termeni	20
	Resurse utile	21





Kit de acțiune pentru adolescenți

Știai că în luna mai 2018 va intra în vigoare un **Regulament privind Protecția Generală a Datelor (General Data Protection Regulation – GDPR)**¹ în legislația tuturor țărilor Uniunii Europene? Vestea bună este că acest Regulament își propune să îți protejeze **intimitatea și datele personale** pe Internet asigurându-se că furnizorii de social media și servicii informaționale:

- tratează datele tale în **mod transparent și corect**
- nu mai transferă datele personale către **terți** fără consimțământul tău explicit
- îți respectă **“dreptul de a fi uitat”**
- nu mai colectează date ale **minorilor** și nu le folosesc pe acestea în scop de marketing (*profiling*).

Veștile proaste sunt că, dacă nu acționăm acum, acest Regulament va interzice persoanelor sub 16 ani să acceseze **serviciile societății informaționale** (ceea ce înseamnă social media și multe alte website-uri) dacă aceștia nu au **consimțământul** părinților sau tutorilor (articolul 8)²! Acum imaginează-ți care ar putea fi consecințele acestei măsuri pentru tine dacă ești un adolescent din UE. Nu vei mai putea socializa sau explora site-uri noi sau aplicații decât dacă părintele este de acord de fiecare dată? Și cum rămâne cu consecințele pentru copiii sub 13 ani?

Ai puterea să schimbi acest lucru, deoarece Articolul 8 din GDPR spune:

“Statele Membre pot prevedea prin lege o vârstă mai mică în acest scop, cu condiția ca aceasta să nu fie mai mică de 13 ani.”

Acest Kit de acțiune pentru adolescenți nu își propune doar să te facă să te gândești la drepturile tale pe Internet, ci îți oferă și posibilitatea de a te asigura că vocea ta este auzită de către legislatorii și factorii de decizie de la nivel național.

Cum? Postează-ți creațiile și feedback-ul privind activitățile din acest kit pe platforma de socializare preferată (care acceptă hashtag-uri, și anume Facebook, Google+, Instagram, Pinterest, Tumblr sau Twitter) înainte de data de 15 decembrie 2017. Lucrările tale vor fi trimise către legiuitorii de la nivel național și european și vor contribui la dezvoltarea unui ghid privind drepturile pe internet și a unei carte care vor fi lansate public în lunile ianuarie și februarie 2018. Pentru a putea să urmărim toate mesajele și creațiile, te rugăm să le publici pe acestea utilizând **hashtag-ul #ParereaTaGDPR**. Dacă adaugi și hashtag-ul **#GDPR** și **#RomaniaGDPR** **#DrepturileCopilului** **#OraDeNet**, ideile tale vor ajunge la chiar mai multe persoane.

Nu uitați să setați opțiunea “Vizibil pentru public/oricine” pentru postările cu care doriți să contribuiți la inițiativa GDPR pentru ca ele să poată fi identificate. Dacă aveți nevoie de informații suplimentare, scrieți-ne la ajutor@oradenet.ro

Profesorii, liderii de tineret etc. pot găsi informații utile și un glosar pe ultimele pagini ale kit-ului.

1 <http://www.privacy-regulation.eu/ro/>

2 <http://www.privacy-regulation.eu/ro/8.htm>



Spune-ți
părererea!

1. Susține-ți drepturile

Activitatea 1 Cunoașterea drepturilor tale!

Declarația Universală a Drepturilor Omului¹ adoptată în 1948 de Națiunile Unite este valabilă pentru toate persoanele, indiferent de naționalitate, religie, rasă sau vârstă. Copiii au aceleași drepturi ale omului ca adulții. Însă, pentru că sunt mai vulnerabili decât adulții, au nevoie și de îngrijire specială și protecție. Drepturile lor au fost definite în cadrul unei Convenții speciale a Națiunilor Unite (UNCRC)² semnată de aproape toate statele din lume de la intrarea acesteia în vigoare în 1989. Conform Articolului 12 din UNCRC, copiii au dreptul de a-și cunoaște drepturile și de a fi împuterniciți să acționeze în vederea promovării și protecției acestor drepturi. Scrie și încearcă să ilustrezi câteva drepturi speciale pe care consideri că copiii și adolescenții trebuie să le protejeze. Ce responsabilități sunt legate de aceste drepturi?

Activitatea 2 Creează un meme cu drepturile tale

Câte dintre drepturile protejate de UNCRC poți enumera? Dacă nu ești sigur de drepturile tale, citește o scurtă versiune a acestei convenții la adresa http://salvaticopiii.ro/upload/p000600010000_Conventia_ONU_pentru_copii_2010.pdf. Care dintre drepturile tale pot fi prejudiciate dacă ai avea nevoie de consimțământul părinților sau tutorelui tău de fiecare dată când îți dorești să utilizezi un nou serviciu de social media sau Internet care colectează date personale? Care dintre drepturile părinților tăi ar fi prejudiciate?

Alege un partener sau un grup mic cu care să lucrezi și notați 5 drepturi care sunt cu precădere importante pentru voi și care considerați că ar trebui protejate cel mai mult în lumea de azi. Creați un **meme** pentru unul sau două dintre cele 5 drepturi definite. Mai multe informații despre cum să crezi un meme la: <https://www.digitaltrends.com/social-media/how-to-make-your-own-meme/>.

Activitatea 3 Exerciță-ți drepturile online³

Drepturile omului se aplică în aceeași măsură și offline și online. În 2012, Consiliul Națiunilor Unite pentru Drepturile Omului a făcut o afirmație istorică⁴ cum că aceleași drepturi pe care le au oamenii offline trebuie protejate și online.

Promovarea și asigurarea drepturilor digitale ale tinerilor sunt importante pentru un mediu online mai incluziv. Discută împreună cu partenerul tău despre ce înseamnă aceste drepturi în practică în contextul Internetului. Care dintre aceste drepturi vă afectează în orice fel intimitatea sau datele personale? Creați un poster prin care să exemplificați modul în care vă puteți exercita drepturile online. Pentru a crea un poster, verifică următoarele modalități gratuite de a crea un poster online:

<http://listoffreeware.com/list-of-free-online-poster-makers/>.

1 http://salvaticopiii.ro/upload/p000600010000_Declaratia%20universala%20a%20drepturilor%20omului.pdf
<http://www.youthforhumanrights.org/what-are-human-rights/universal-declaration-of-human-rights/articles-1-15.html>
https://en.wikipedia.org/wiki/Universal_Declaration_of_Human_Rights

2 http://salvaticopiii.ro/upload/p000600010000_Conventie_ONU_drepturile_copilului_2010.pdf
<http://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx>

3 <http://5rightsframework.com/>

4 <https://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/20/L.13&Lang=E>



Spune-ți
părererea!

2. Provocări iminente

Articolul 8¹ din GDPR, care va fi adoptat în toate Statele Membre ale Uniunii Europene în 2018, indică vârsta de 16 ani ca vârsta minimă la care tinerii pot decide ei înșiși dacă să acceseze "servicii ale societății informaționale". Până la această vârstă, vor avea nevoie de permisiunea părintelui sau tutorelui!

Activitatea 1 Spune-ți părerea!

Într-un grup mic, împărtășește ce crezi despre această restricție în funcție de vârstă. Scrieți pe bilețele diferitele emoții pe care le-ați manifesta dacă ar trebui să cereți permisiunea părintelui (părinților) sau tutorelui pentru a utiliza anumite site-uri pe Internet. Cum te-ai simți să îți sâcâi părinții pentru a-ți permite să creezi un cont Facebook, să instalezi o aplicație sau să te abonezi la un serviciu online? Ce crezi despre capacitatea părinților tăi de a înțelege funcționarea *serviciilor societății informaționale și despre responsabilitatea pentru intimitate și datele personale?*

Strângeți toate bilețelele și fotografiați-le.

Activitatea 2 Găsește un echilibru

Încearcă să reflectezi asupra impactului pe care GDPR l-ar putea avea asupra drepturilor tale online. Ce activități online, oportunități educaționale și sociale va afecta cel mai mult? Ia în considerare consecințele în context școlar și pentru tinerii creatori și dezvoltatori online.

Discută despre modalitățile de a asigura dreptul copiilor la protecție, în același timp respectând dreptul la participare. Creează o **hartă cognitivă** care să prezinte ideile tale cu privire la aceste aspecte. Pentru a crea o hartă cognitivă, verifică software-ul gratuit de mind mapping la <https://cloudsmallbusinessservice.com/blog/best-open-source-mind-mapping-software-254388.html>.

Activitatea 3 Ascunde sau șterge?

În prezent, 38% dintre tinerii între 9 și 12 ani au deja propriul profil pe un site de socializare (social networking site - SNS)². Dacă unii părinți nu și-ar da consimțământul pentru tinerii între 13 și 16 ani? Împreună cu un partener, sau într-un grup mic, discutați eventualele consecințe ale condiției din cadrul GDPR de a avea consimțământul părinților asupra comportamentului tinerilor și posibilele implicații pentru siguranța acestora. Dar tinerii care și-au dezvoltat profilurile SNS de câțiva ani deja? Creează câteva benzi desenate prin care să îți prezinți ideile. Verifică următoarele aplicații și instrumente web prin care îți poți crea propriile benzi desenate: <http://www.educatorstechnology.com/2017/05/some-of-best-web-tools-and-mobile-apps.html>

Activitatea 4 Te simți neajutorat?

Toți tinerii ar trebui să aibă acces facil la ajutor și sfaturi oricând au nevoie. Pe lângă liniile de **consiliere**³ specializate, susținerea reciprocă joacă un rol important pentru mulți tineri care se găsesc în situații problematice. Discută acest aspect împreună cu un partener sau într-un grup mic și scrie pe bilețele diferitele restricții pe care GDPR îți le poate aduce în această privință. Apoi fotografiază toate aceste bilețele.

1 <http://www.privacy-regulation.eu/ro/8.htm>

2 [http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%2011%20\(2009-11\)/EUKidsOnlineReports/ShortSNS.pdf](http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%2011%20(2009-11)/EUKidsOnlineReports/ShortSNS.pdf)

3 <http://www.oradenet.salvaticopiii.ro/ctrl-ajutor>



Spune-ți
părererea!

3. Cu un pas în viitor

Activitatea 1 Lasă-te cuprins de o lume captivantă

Realitatea Virtuală este tot mai populară și ne oferă o experiență captivantă cu totul nouă. Și, contrar opiniei majoritare, VR nu înseamnă doar jocuri. Există tot mai multe aplicații VR care oferă experiențe educaționale de neuitat.

Ai încercat până acum Realitatea Virtuală? Dacă da, împreună cu un partener, împărtășiți-vă impresiile. Dacă nu, informează-te pentru a găsi răspunsurile la câteva dintre următoarele întrebări. Cum poate afecta VR drepturile noastre, inclusiv protecția datelor personale? Ce oportunități aduce? Cum poate afecta posibilitățile de învățare și colaborare?

la în considerare și riscurile. De ce stabilesc limite de vârstă producătorii de dispozitive VR? Creează câteva benzi desenate care să illustreze opiniile tale asupra subiectului de mai sus. Verifică următoarele aplicații și instrumente web prin care îți poți crea propriile benzi desenate: <http://www.educatorstechnology.com/2017/05/some-of-best-web-tools-and-mobile-apps.html>.

Activitatea 2 Fii un pilot inteligent!

Tehnologia cu **drone** s-a îmbunătățit tot mai mult în ultimul timp și aceste mici vehicule fără pilot sunt în prezent printre cele mai populare cadouri pentru copii. Asumarea rolului de pilot și dirijarea unei drone poate fi distractivă, dar sunt și câteva lucruri importante legate de siguranță ce ar trebui avute în vedere. Anumite drone au camere și permit **aplicații de urmărire**. Discută cu un partener sau într-un grup mic aspectele legate de intimitate pe care le implică acest lucru. Cum pot dronele invada intimitatea altor persoane? Notați 5 sfaturi privind utilizarea responsabilă a dronelor. Pentru informații privind siguranța dronelor, verifică <http://dronerules.eu>, materialul video la https://youtu.be/5Xs_eVx4nuw și posterul la <http://dronerules.eu>, the video at https://youtu.be/5Xs_eVx4nuw and the poster at https://www.easa.europa.eu/system/files/dfu/213888_EASA_DRONE_POSTER_v5.pdf.

Poți obține informații și sfaturi foarte utile privind dronele la https://www.easa.europa.eu/system/files/dfu/Q%26A_Commission_Drones.pdf.

Activitatea 3 Selfie din mers

Dacă privești imaginea „Internetul într-un minut” de pe pagina următoare, vei vedea că în fiecare minut se fac 1,8 milioane de instantanee în întreaga lume și multe dintre acestea este foarte posibil să fie selfie-uri. Milioane de fotografii de tip selfie sunt postate în fiecare zi pe diferite platforme de socializare. Selfie-urile reprezintă aproape 1/3 din toate fotografiile făcute de tinerii din grupa de vârstă 18-24 de ani, conform statisticilor oferite de Samsung¹. Te-ai gândit vreodată la impactul pe care îl poate avea acest lucru asupra imaginii noastre de sine, autenticității noastre? Pot fi selfie-urile utilizate pentru a crea o imagine de sine, identitate și reputație pozitive?

Gândește-te acum la aspectele legate de intimitate și reputație online pe care le pot ridica selfie-urile. Ține minte că nu doar Facebook și Snapchat permit partajarea fotografiilor, ci și diferite dispozitive conectate, care apoi încarcă și stochează fotografiile de tip selfie pe servere ale companiilor! Nu uita că o fotografie poate să îți dezvăluie și locația fizică! Reflectează asupra riscurilor la care îi expun părinții pe copiii lor când încarcă imagini ale lor. Lucrează într-un grup mic pentru a crea 2 sau 3 **meme-uri** pentru a-ți împărtăși ideile. Mai multe informații despre cum să creezi un meme: <https://www.digitaltrends.com/social-media/how-to-make-your-own-meme/>.

1 <http://www.samsung.com/za/news/local/samsung-selfie-campaign-wins-african-excellence-award/>

2017 *This Is What Happens In An Internet Minute*

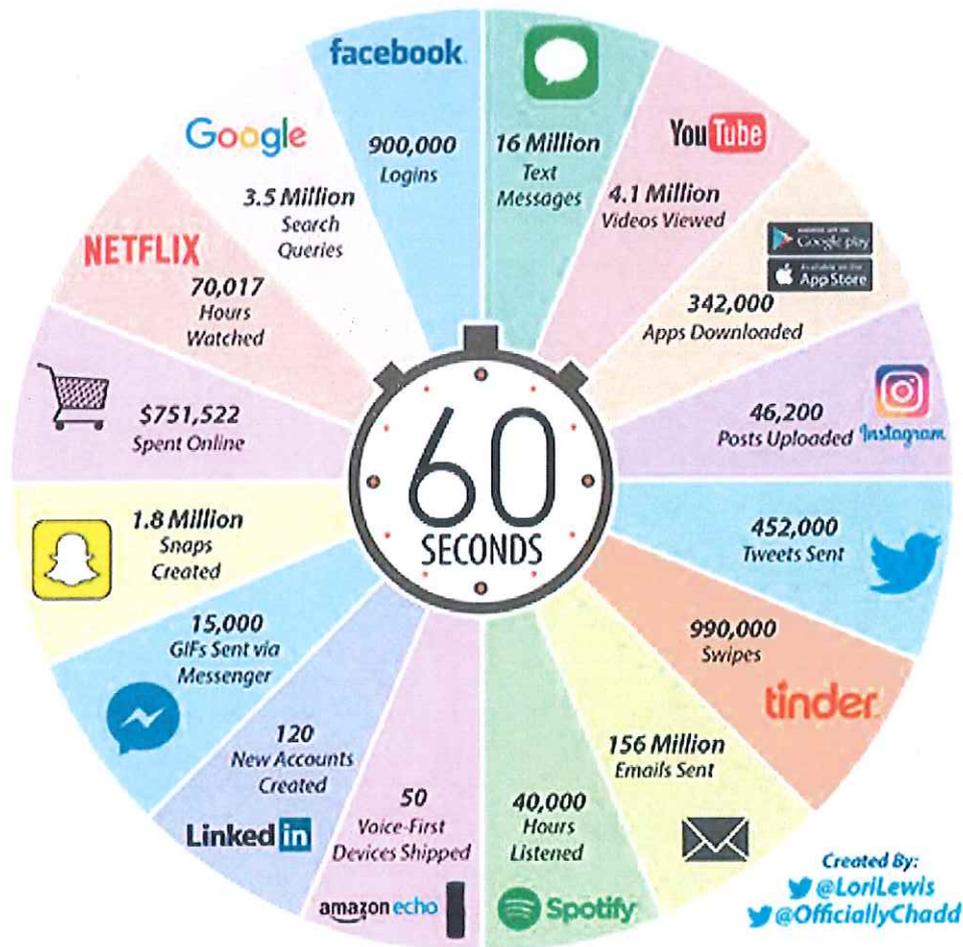


Figura 1: Ce se întâmplă în 60 de secunde pe Internet (<http://thebln.com/2017/03/happens-every-minute-internet-2017/>)

Activity 4 Jucării Smart?

În prezent există deja 14 miliarde de dispozitive de tip „Internetul Obiectelor” (Internet of Things) conectate. Se preconizează că vor exista în jur de 50 de miliarde de dispozitive conectate în lume până în 2020². Este posibil să deții deja un dispozitiv portabil, cum ar fi un tracker de fitness sau ceas smart. Poți să dai mai multe exemple de asemenea dispozitive?

Internetul Obiectelor (Internet of Things – IoT) ridică multe probleme legate de intimitate, iar jucăriile conectate, în special, prezintă un set cu totul nou de provocări în ceea ce privește drepturile copiilor. Recent, s-au raportat mai multe cazuri în care înregistrări de voce și informații personale ale copiilor au fost făcute publice din cauza jucăriilor de tip IoT. O conversație cu un ursuleț de pluș conectat nu este o doar o conversație cu o jucărie, copilul vorbește cu corporația care a produs jucăria!

Cum pot aceste dispozitive să încalce anumite drepturi ale utilizatorilor și ce se întâmplă cu datele personale pe care le colectează? În ce mod pot expune la riscuri și informațiile despre adulți? Discută într-un grup mic de ce ar trebui să fie conștienți părinții copiilor mici. Nu uitați să luați în considerare aspectele legate de dezvoltarea

² <http://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated>

copiilor și emoțiile acestora când interacționează cu un robot conectat. Scrieți 5 sfaturi privind măsurile de precauție pe care ar trebui să le ia părinții și tutorii când cumpără jucării conectate la Internet.

Activitatea 5 VIDEO-net

Se estimează că până în 2020 un procent covârșitor de 80% din traficul pe Internet va fi de tip conținut video. Conținutul video reprezintă deja 64% din tot conținutul web în SUA³.

Potențialul pentru acest tip de conținut este enorm. Deși revoluționează Internetul, va avea un impact și asupra drepturilor și responsabilităților noastre. Cum putem crea spații online bazate pe respect și încredere?

Într-un grup mic, creați o **hartă cognitivă** care să prezinte diferitele aspecte etice legate de crearea sau chiar simpla vizualizare a materialelor video online. Gândiți-vă la subiect din perspectiva creatorilor, dezvoltatorilor și contribuitorilor, precum și a utilizatorilor care postează conținut. Ți, în cele din urmă, ce reguli ar trebui să stabilească furnizorii de servicii, cum ar fi YouTube și Facebook? Pentru a crea o hartă cognitivă, verifică software-ul gratuit de mind mapping la <https://cloudsmallbusinessservice.com/blog/best-open-source-mind-mapping-software-254388.html>.

Sugestie privind activitatea: Încearcă să creezi un scurt clip video fără a arăta imagini ale unor persoane. Este posibil să ți se pară utile InstaLive sau Musical.ly.

Activitatea 6 Turnul Babel pe Internet

Lumea online nu este cu siguranță un spațiu foarte echilibrat când vorbim de limba conținutului. Din cele aproximativ 6.000 de limbi utilizate în lume în prezent, cele mai populare zece limbi reprezintă 82%⁴ din conținutul online. Un studiu din 1997 arăta că 80% din conținutul www era în limba engleză; în prezent, se consideră că limba engleză reprezintă aproximativ 55%, cu doar 6,19% din conținut în limba rusă, de exemplu, și 4,4% în chineză.

Ce ar putea însemna acest lucru pentru vorbitorii de alte limbi? Cum afectează cele de mai sus dreptul nostru de a vorbi limba noastră națională și de a ne manifesta propria cultură? Pe de altă parte, gândește-te și la sprijinul pe care îl oferă Internetul pentru persoanele care învață limbi străine. Într-un grup mic, creați un poster prin care să explicați provocările și oportunitățile în acest domeniu. Pentru a crea un poster, verifică următoarele modalități gratuite de a crea un poster online: <http://listoffreeware.com/list-of-free-online-poster-makers/>.

³ <http://www.smartinsights.com/digital-marketing-platforms/video-marketing/video-account-80-internet-traffic-2020-chartoftheday/>

⁴ <https://www.language-testing.com/blog/commercial/the-digital-language-divide>



Spune-ți
părererea!

4. E timpul de acțiune!

Drepturile omului sunt cel mai bine respectate și apreciate atunci când le cunoaștem, le susținem și le aplicăm în viața noastră. Acestea nu pot fi protejate doar prin măsuri legale. Ele trebuie protejate și respectate de toată lumea, inclusiv de copii și de tineri. Deși textul final al GDPR a fost adoptat, nu este încă prea târziu să acționăm! Regulamentul se aplică doar începând cu luna mai 2018. Înainte de această dată, Statele Membre ale UE trebuie să pregătească linii directoare clare privind implementarea, inclusiv aspectul legat de consimțământul părinților. Pentru a face acest lucru corect, trebuie să se asigure că liniile directoare sunt **bazate pe dovezi** și că toate părțile implicate au fost consultate, în special tinerii, deoarece ei sunt aceia ale căror oportunități GDPR le poate afecta semnificativ.

Alătură-te altor tineri europeni în crearea unui ghid online cu privire la drepturile tale pe Internet; tu și alții veți putea utiliza conținutul pentru a fi siguri că vocea voastră se face văzută tare și clar! Conform articolului 12¹ din UNCRC, copiii au dreptul de a fi ascultați în toate aspectele care îi vizează. Această este oportunitatea ta de a-ți exercita dreptul la participare și libertate de expresie!

Îți poți încărca creațiile pe Instagram, Facebook, Google+, Instagram, Pinterest, Tumblr sau Twitter, utilizând unul dintre cele trei hashtag-uri: #ParereaTaGDPR, #GDPR sau #DrepturileCopilului. Prin ideile tale, vei putea stârni interesul altor adolescenți europeni și trezi publicul pentru a realiza impactul pe care îl va avea GDPR asupra drepturilor copiilor. Ele vor prezenta și câteva dintre provocările mai mari cu care trebuie să se confrunte copiii în mediul online în prezent. Cei mai proactivi contribuitori la ghid vor fi invitați să ajute la dezvoltarea unei carte a drepturilor online pe baza conținutului. Aceasta va evidenția cele mai importante drepturi digitale identificate de tinerii europeni pe măsură ce GDPR începe să provoace efecte în viața lor.

Activitatea 1 Planifică o campanie

Acum este momentul să îți lași creativitatea să zboare și să îți faci vocea auzită! Într-un grup, creați un poster și dezvoltați un slogan care să vă protejeze drepturile care pot fi afectate ca urmare a obligației din GDPR de a avea consimțământul părinților. Pentru a crea un poster, verifică următoarele modalități gratuite de a crea un poster online: <http://listoffreeware.com/list-of-free-online-poster-makers/>.

Activitatea 2 Vino cu soluții

Furnizorii de servicii ale societății informaționale joacă un rol important în a se asigura că participarea online a tinerilor este cât mai sigură posibil. Ar trebui să ți se ofere instrumente care să te ajute să faci alegerile corecte cu privire la intimitatea și siguranța ta. Împreună cu un partener sau într-un grup mic, veniți cu câteva soluții privind siguranța, care ar putea fi implementate în locul pragului de vârstă de 16 ani pentru consimțământul părinților. Creați două sau trei **meme-uri** pentru a vă prezenta ideile. Poți găsi mai multe informații despre cum să crezi un meme la <https://www.digitaltrends.com/social-media/how-to-make-your-own-meme/>

¹ http://salvaticopiii.ro/upload/p000600010000_Conventie_ONU_drepturile_copilului_2010.pdf

Activitatea 3 Acționează la nivel local

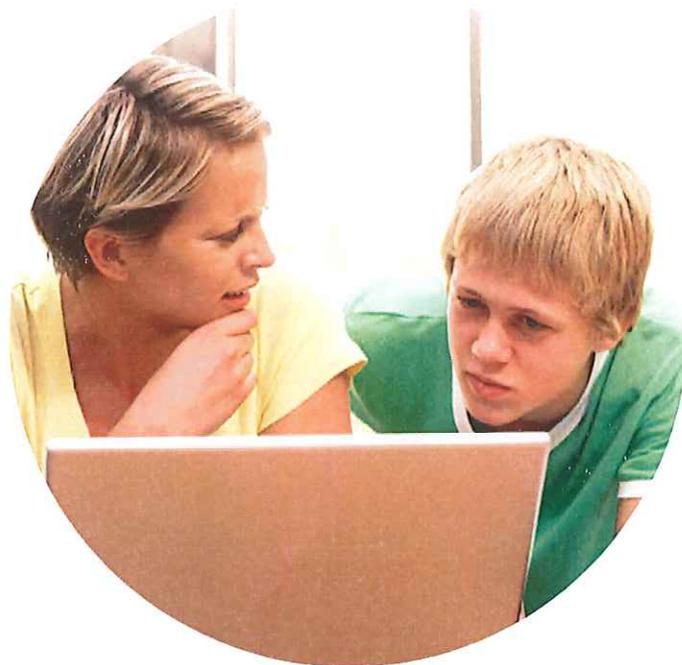
În grup, gândiți-vă la idei prin care puteți deschide subiectul drepturilor digitale ale copiilor la școală sau în comunitățile voastre locale și online. Nu uita că acțiunile locale se traduc în efecte globale! Iată câteva idei:

- Organizați o dezbateră privind impactul GDPR cu câțiva prieteni și colegi de clasă, care să fie susținută la școală sau în comunitate.
- Discutați cu profesorii utilizând ICT la clasă, pentru a le explica problemele care vor apărea și discutați cu aceștia modurile în care vă pot sprijini eforturile.
- Prezentați un workshop părinților privind drepturile digitale ale tinerilor.
- Identificați o organizație centrată pe tineri în zona voastră și discutați această problemă.
- Faceți lobby la parlamentarii europeni pentru a le obține sprijinul.
- Contactați media la nivel local pentru a le atrage atenția asupra subiectului și pentru a vă ajuta să atrageți noi susținători.

Activități de reflecție de la egal la egal – pentru profesori și lideri ai tinerilor

De multe ori copiii și tinerii nu își cunosc drepturile. În calitatea noastră de profesori, lideri ai tinerilor și părinți, trebuie să îi încurajăm să se gândească la drepturile lor, provocările cu care se confruntă atât în mediul online cât și offline și ce pot face ei când drepturile lor nu sunt respectate. Acest kit a fost creat pentru a fi utilizat în context peer-to-peer și oferă multe idei pentru activități și acțiuni pe care copiii și tinerii le pot întreprinde în școală și comunitate. În afară de încurajarea reflecției asupra tehnologiilor inovatoare care vor continua să schimbe radical modul în care gândim, acționăm și interacționăm, activitățile propuse vor ajuta și la inițierea discuției privind măsurile alternative la cele prevăzute de GDPR pentru protejarea intimității și a datelor personale ale tinerilor și încurajarea acestora să acționeze.

Deși majoritatea activităților necesită aproximativ 30 - 40 de minute, unele pot acoperi mai multe lecții. Alegeți liber activitățile pe care le considerați cele mai adecvate pentru tinerii cu care lucrați, sau lăsați-i pe ei să aleagă activitățile care îi interesează cel mai mult. Împreună, puteți face diferența pentru generația de azi și generațiile care vor urma.



Glosar de termeni



A intra în vigoare - începe să se aplice, să devină valabilă

Consimțământ - permisiune

Dronă - un aparat de zbor fără pilot controlat la distanță de cineva de pe pământ, denumit și vehicul aerian fără pilot (unmanned aerial vehicles - UAVs) sau sisteme de zbor fără pilot (unmanned aircraft systems - UASes)

State Membre ale UE - țări care sunt membre ale Uniunii Europene

Bazat pe dovezi - susținut de studii științifice

Regulamentul privind Protecția Generală a Datelor (GDPR) - un cadru legal care stabilește linii directoare pentru colectarea și procesarea informațiilor personale ale persoanelor din Uniunea Europeană

Hashtag - un cuvânt sau o frază precedate de simbolul # care clasifică sau împarte în categorii textul însoțitor (cum ar fi un tweet). Mai multe informații privind hashtag-urile la <https://spark.adobe.com/blog/2016/11/30/what-you-need-to-know-about-hashtags/>

Linii de consiliere - servicii de ajutor și sprijin pentru copii, unde pot discuta despre problemele care îi îngrijorează și primi consiliere profesională

Drepturile omului - drepturile fundamentale de care beneficiază oamenii datorită faptului că sunt ființe umane; sprijinite prin mai multe declarații internaționale

ICT - tehnologia informației și comunicării

Internetul Obiectelor (Internet of Things - IoT) - un concept în care obiectele fizice de uz zilnic sunt conectate la Internet și pot comunica cu alte dispozitive

Meme - un meme partajat online poate fi aproape orice partajat voluntar, inclusiv fraze, imagini, zvonuri sau fișiere audio sau video. Mai multe informații despre cum poate fi creat un meme: <https://www.digitaltrends.com/social-media/how-to-make-your-own-meme/>

MEP - membru al Parlamentului European

Hartă cognitivă - o diagramă pentru reprezentarea conceptelor, ideilor și conexiunilor între acestea

Minori - o persoană sub o anumită vârstă (în general 18 ani), considerată prin lege că este prea tânără să aibă responsabilitățile legale ale unui adult

Date personale - date legate de o persoană care poate fi identificată, localizată sau contactată prin intermediul acestor date

Intimitate - dreptul unei persoane de a-și păstra subiectele personale secrete și fără a fi supravegheate

Dreptul de a fi uitat - un concept conform căruia o persoană are dreptul de a solicita să îi fie eliminate informațiile personale de pe Internet

Terță parte - cineva care ar putea fi indirect implicat, dar nu este un factor de interes principal

Aplicație de urmărire - o aplicație care permite urmărirea locației cuiva

Realitate virtuală - o lume artificială de imagini și sunete create prin intermediul unui software pe calculator

Resurse utile



<http://www.oradenet.ro>

Ora de net este un program european unic în România, care promovează siguranța pe Internet pentru copii și adolescenți.

<http://ec.europa.eu/justice/data-protection/> - pentru mai multe informații despre Regulamentul privind Protecția Generală a Datelor. Alte informații utile sunt disponibile la https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

<http://www.privacy-regulation.eu/ro/8.htm> - informații despre articolul 8 din GDPR

<https://www.betterinternetforkids.eu/> - informații și resurse din rețeaua Insafe care își propune să facă Internetul un loc mai bun pentru copii și adolescenți

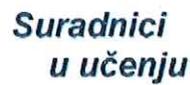
<http://blogs.lse.ac.uk/mediapolicyproject/2016/03/01/eu-general-data-protection-regulation-article-8-has-anyone-consulted-the-kids/> - un blog postat de un expert britanic cu privire la eventualele efecte ale GDPR

<http://www.webwewant.eu> - activități pe teme de actualitate, inclusiv intimitate, creativitate, eu în online/offline create de adolescenți pentru adolescenți, cu planuri de lecții pentru profesori

<https://www.youtube.com/watch?v=PwrZtkmGS30> - un material video de la Pantallas Amigas* (în limba spaniolă) despre dreptul copiilor/adolescenților de a-și exprima opiniile cu privire la deciziile care le afectează activitatea pe Internet

<https://www.youtube.com/watch?v=G1kEUPQjJfo> - un material video de la Pantallas Amigas* (în limba spaniolă) care ilustrează modul în care GDPR ar putea afecta intimitatea, deoarece vorbește despre imagini integrate pentru geolocație

*Pot fi subtitrate în alte limbi la cerere



#ParereaTaGDPR #RomaniaGDPR #DrepturileCopilului #OraDeNet

