

DREPTURILE COPIILOR



Dorim să protejăm copii în mediul online, focusându-ne asupra temelor de mai jos pentru a consolida drepturile acestora în era digitală:

- **DREPTUL LA IDENTITATE ȘI CONFIDENȚIALITATE**
Astăzi, cunoștințele despre viața privată și protecția propriilor date sunt mai importante decât oricând.
- **DREPTUL LA INFORMARE ȘI DREPTUL DE PARTICIPARE**
Este important să găsim echilibrul între protecție și participare. Protecția tinerilor împotriva conținutului dăunător online nu ar trebui să restricționeze dreptul copiilor la participare și la informație.
Tehnologiile de cenzură, filtrare sau blocare nu ar trebui înțelese ca o "remediere perfectă" pentru a proteja copiii de problemele online. Împuternicirea copiilor să folosească în mod independent mijloacele digitale în condiții de siguranță și în scopuri proprii necesită îndrumări și sprijin din partea adulților. Participarea online este o parte fundamentală a societății moderne. Copiii și tinerii trebuie să aibă posibilitatea de a influența procesul de luare a deciziilor care îi afectează viața.
- **DREPTUL LA LIBERTATEA EXPRESIEI, ALEGERE ȘI JOACĂ**
Mediile digitale sunt pline de oportunități de a juca, de a se distra, de a se întâlni cu prietenii și de a dezvolta abilități digitale. Prin aceste activități, copiii au posibilitatea de a se dezvolta fizic, mental, emoțional și social. Astfel de activități îi pot ajuta să învețe cum să trăiască într-o societate digitală în schimbare rapidă. Dorim ca copiii să se angajeze în activități de joacă și agrement adecvate vârstei lor. Este dreptul copiilor să se adune online pentru comunicare și exprimare.

- **DREPTUL DE A FI SIGUR ȘI PROTEJAT DE TOATE FORMELE DE VIOLENȚĂ**
Protejarea copiilor împotriva daunelor și a riscurilor în mediile online va fi întotdeauna una dintre principalele noastre priorități.
O relație strânsă, cu discuții deschise între copil și adulți, protejează copiii de rău. Copiii au nevoie de îndrumări în ceea ce privește modul de protejare online, ce comportament este adecvat față de ceilalți și ce comportament este acceptabil față de ei înșiși.
- **DREPTUL LA SĂNĂTATE ȘI BINE**
Digitalizarea societăților afectează sănătatea și bunăstarea copiilor: impact pe care abia începem să-l înțelegem.
Este important să conștientizăm impactul, să prevenim și să atenuăm efectele potențial dăunătoare pe care tehnologia digitală le poate avea asupra sănătății și bunăstării copiilor și să căutăm în mod activ oportunități de îmbunătățire a sănătății copiilor folosind noile tehnologii.

RISCURILE LA CARE POT FI SUPUȘI COPIII LA ACCESAREA ANUMITOR TIPURI DE INTERNET NEFILTRAT

Internetul a devenit în ultimii ani canalul de informare cel mai folosit de tineri. Din ce în ce mai mulți copii dețin un smartphone sau o tabletă și accesează Internetul oriunde s-ar afla. Mobilitatea împiedică părinților să fie vigilenți în contextul în care numărul site-urilor pentru adulți, jocurile de noroc sau violente cresc, un minor îl poate accesa ușor cu câteva clicuri.

Copiii și adolescenții sunt supuși unor riscuri precum:

- Expunerea la conținut ilegal și/sau dăunător;
- Victimizarea prin intimidare, hărțuire sau amenințare (sau "cyberbullying");
- Instrăinarea sau furtul datelor cu caracter personal;
- Trimiterea sau primirea de secvențe video, imagini sau mesaje cu caracter sexual (sau "sexting");
- Grooming (ademenirea în scopul săvârșirii actelor sexuale);
- Identitatea, reputația online și securitatea pe internet;
- Informații neverificate;
- Utilizarea excesivă a calculatorului sau dependența de jocuri și Internet;
- Raportarea conținutului ilegal/ dăunător.

Cyberbullying – hărțuirea online



Cyberbullying este o formă de hărțuire. Este un act agresiv care utilizează diferite forme de comunicare electronică (rețele sociale, smartphone, computere, tablete, chat, site-uri web) pentru a amenința, a insulta intenționat și repetat o victimă. Ea este realizată de un individ sau de un grup de indivizi. Cyberbullying se practică prin e-mailuri, telefoane mobile, rețele sociale, site-uri de partajare a fotografiilor, mesagerii instantanee, forumuri, chat-uri, jocuri online etc. Acestea sunt acte de violență și se fac în scopul amenințării, intimidării sau insultării victimelor. De exemplu:

- crearea unui profil fals, trimiterea de mesaje insultătoare repetitive răspândind zvonuri nefondate,
- postare de fotografii compromițătoare sau video umilitoare, insultarea foarte violent, creând zvonuri (într-un grup sau într-o rețea socială) împotriva unui alt elev, etc ...
- excluderea cu rea-voință a unei persoane dintr-un grup sau o comunitate online;
- furtul de parole pentru a avea acces la corespondența personală și a transmite în numele victimei mesaje compromițătoare;
- trimiterea intențională a unui mesaj virusat.

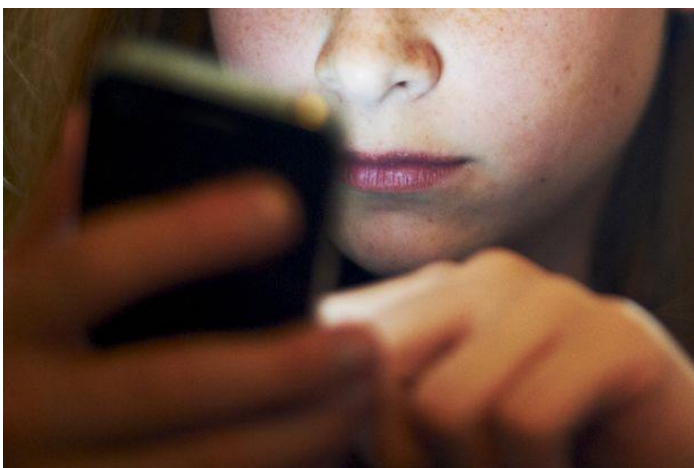
Hărțuirea online este deosebit de periculoasă mai ales pentru că este constantă, publică și greu de evitat de către victime. Poate avea loc oricând – la școală sau acasă - și poate implica grupuri mari de copii.

SFATURI:

- Asigurați-vă că copiii împărtășesc cu Dvs. ce li se întâmplă. Copiii trebuie să le spună părinților, profesorilor sau altor adulți de încredere dacă sunt hărțuiți online. Explicațiile copiilor că nu înseamnă că părăsesc, ci că își apără dreptul de a fi protejat.
- Oferiți-le sfaturi despre cum să reacționeze când sunt hărțuiți. Deși ar putea fi tentați să facă acest lucru, copiii nu trebuie să se răzbune niciodată pe cei care-i hărțuiesc. În schimb, copiii trebuie să adune toate dovezile de hărțuire (emailuri, imagini, mesaje etc.) și să nu le șteargă.

- Reamintiți-le copiilor să nu-și dezvăluie parolele prietenilor lor. O formă des întâlnită de hărțuire online apare atunci când copiii își dezvăluie parolele, se conectează pe conturile altor copii și se dau drept copiii respectivi. Copiii se pot proteja conștientizând faptul că parolele sunt strict secrete și că acestea pot fi spuse doar părinților.
- Ajutați copiii să seteze o parolă sigură. O parolă puternică și sigură, ușor de amintit însă greu de ghicit de către alte persoane, trebuie să conțină minimum 10 caractere, dintre care cel puțin o majusculă, cel puțin o minusculă, precum și numere și simboluri. Nu este indicată alegerea unor citate cunoscute sau a unor sloganuri și cuvinte uzuale. Politica de securitate trebuie să includă schimbarea periodică a parolelor.

Sexting



Sexting-ul este definit ca transmiterea de mesaje sau imagini cu conținut sexual explicit, cel mai adesea prin intermediul telefonului mobil. Adolescenții și tinerii trimit texte, fotografii sau secvențe video cu caracter sexual, în care protagoniștii sunt de cele mai multe ori ei înșiși, prin SMS, email, webcam. Aceste medii sunt arhivate și pot fi difuzate masiv și necontrolat.

RISCURILE SEXTING-ULUI:

- 1. Pierderea intimității:** când fișierul este trimis, nu mai puteți controla distribuția acestuia. El poate nimeri în mâinile oricărei persoane.
- 2. Tulburări psihologice:** prezentarea intimității în fața celorlalți poate provoca probleme cum ar fi depresia, excluderea din cercul social etc.
- 3. Hărțuirea virtuală:** dacă colegii descoperă fotografiile sau videoclipurile sexuale pe care le-ai trimis, te pot umili și pot inunda cu comentarii negative.
- 4. Extorcare:** fișierul poate fi folosit pentru a șantaja persoana implicată, forțându-i să facă anumite lucruri, astfel încât părinții, profesorii sau prietenii săi să nu fie conștienți de existența acestui videoclip sau a acestui imagine.

Prin urmare, este foarte important să acordăm atenție acestui fenomen. Nu este un joc simplu, deoarece integritatea fizică și psihologică a unui adolescent poate fi modificată.

CE AR TREBUI SĂ FACĂ PĂRINȚII?

1. În primul rând, ei trebuie să acorde atenție utilizării tuturor tipurilor de dispozitive electronice din posesia copiilor lor.
2. Discutați cu ei despre pericolele la care aceste comportamente îi pot expune. Mai presus de toate, ar trebui să se acorde atenție oricăror schimbări în atitudinea adolescenților, care ar putea dezvălui că s-a întâmplat ceva.
3. Amintiți-le că nimic din ceea ce ei postează pe Internet nu este privat. Odată ce a fost apăsat butonul "Trimite", nu mai este posibilă oprirea răspândirii aceluși conținut.
4. Adresați-vă persoanei care a răspândit fotografia sau secvența video cerându-i să elimine fișierele atât de pe site-ul pe care au fost încărcate cât și de pe dispozitivele pe care se pot afla (telefonul mobil, memorii externe, hard-diskuri).
5. Fiți atent la evoluția emoțională și comportamentală a victimei, iar la nevoie cereți suportul specialiștilor.

Prin urmare, este important să acordăm atenție acestui fenomen și să fim atenți. După cum spune proverbul popular, "prevenirea este mai bună decât vindecarea".

Necunoscuți online



Copiii pot discuta online cu persoane, chiar dacă nu le cunosc. Ei nu îi percep mereu ca pe niște străini, dar îi pot face vulnerabili la agresiuni și prietenii nepotrivite.

Vorbiți despre cine sunt prietenii online, cum își aleg prietenii și ce împărtășesc. O mulțime de copii se bucură de chat online, dar e nevoie să le reamintiți să fie atenți. Oamenii nu sunt întotdeauna cei care pretind că sunt.

Cu copiii mai mici, puteți vorbi despre acest fenomen ca despre un pericol ascuns. Explicați-le care sunt regulile aplicabile online și încurajați-i să vă spună dacă cineva pe care nu-l cunosc solicită să se întâlnească. Discutați cu copiii mai în vârstă despre relațiile sănătoase și încurajați-i să se gândească la ce site-uri vizitează și la ceea ce împărtășesc.

Lăsați copilul să știe că pot să vorbească cu Dvs. sau cu un alt adult în care au încredere, dacă ceva le îngrijorează.

Grooming este atunci când cineva construiește o relație cu un copil pentru a câștiga încrederea lor, cu intenția de a exploata această relație pentru abuz sexual. Poate fi mai ușor online, deoarece groomerul își poate ascunde vârsta, genul și identitatea.

Famiile se tem de multe ori că copiii lor se vor întâlni cu "prieteni" online și vor fi abuzați. Dar copiii pot fi, de asemenea, exploatați prin a fi convinși sau forțați:

- să dețină conversații sexuale prin chat sau prin chat pe web;
- să trimită sau posteze imagini explicit sexuale;
- să participe la activități sexuale prin intermediul unei camere web sau al unui telefon.

Arătați-i copilului ce văd străinii prin căutarea numelui lor când nu sunt conectați. Vorbiți despre asta în contextul vieții reale - ar merge la un străin pe stradă și ar arăta o fotografie din vacanță?

Dacă aveți un copil mic care se joacă online, opriți caracteristicile sociale și de chat. Pe măsură ce se maturizează, vorbiți despre setările de confidențialitate și asigurați-vă că știu cum să blocheze și să raporteze persoanele nepotrivite.

RECOMANDĂRI PRIVIND CONDIȚIILE DE SIGURANȚĂ A COPIILOR ÎN MEDIUL ONLINE



O bună soluție în prevenirea riscurilor online este explicarea pericolelor la care copiii se expun dezvăluindu-și identitatea pe internet persoanelor necunoscute. Acest lucru trebuie făcut de către părinți și în școli, pe înțelesul fiecărei categorii de vârstă, de către fiecare învățător.

Internetul a schimbat în mod spectaculos modul în care copiii interacționează cu lumea. Ei au acces la un volum copleșitor de informații. Cu toate acestea, mediul online, pe lângă beneficiile evidente, comportă în lipsa unei informări corecte și a unei orientări adecvate, riscuri în fața cărora cei vulnerabili sunt în special copiii. În ultimul deceniu, evoluția utilizării Internetului de către copii a fost caracterizată prin două mari direcții, ambele punând în sarcina părinților și a cadrelor didactice un rol crucial în protecția copiilor împotriva riscurilor din mediul online:

- 1) copiii accesează Internetul de la vârste din ce în ce mai mici;
- 2) tehnologia utilizată în acest sens a devenit mobilă și accesibilă oriunde și oricând. Cifrele din întreaga lume demonstrează că mulți dintre copiii preșcolari sunt în măsură să folosească diferite dispozitive de accesare a Internetului și chiar o fac cu sau fără supravegherea părinților.

Telefoanele ”smart” și tabletele, ca dispozitive mobile sunt prevăzute cu tehnologia necesară conectării la Internet, la prețuri din ce în ce mai accesibile. Deși la prima vedere pare a fi o problemă greu de învins, părinții și profesorii pot stabili împreună cu copiii reguli pe care fiecare trebuie să le respecte în utilizarea tehnologiei mobile pentru comunicarea online.

Una din cel mai des întâlnite teme dezbătute în studiile, rapoartele, articolele privind copiii și Internetul este cea a pericolului ca un copil să fie expus accidental sau intenționat unor materiale sau activități ilegale, abuzive, ofensatoare, vulgare ori obscene. Ele pot fi imagini, texte, filme sau fișiere audio. Expunerea la acest tip de conținut poate avea drept consecințe un nivel ridicat de anxietate sau stări traumatiche, ori poate determina prin repetarea expunerii, atitudini de imitare, dezinhibare sau desensibilizare. Copiii intră în contact cu aceste materiale în cele mai multe situații în mod incidental, atunci când sunt în căutare de informații, jocuri, persoane sau locuri. La școală, inclusiv activitățile online cu caracter educațional pot avea ca urmare neplăcută apariția de imagini sau informații ilegale sau dăunătoare. Pentru a evita acest lucru, părinții trebuie să cunoască și să-i informeze pe copii asupra tehnicilor corecte de căutare și asupra procedurilor de apelare a serviciilor specializate (<https://siguronline.md> ; <http://telefonulcopilului.md> ; <https://onlinesafety.info> ; <https://contentfiltering.info> ; <https://safeinternet.org> ; <https://soros.md/publication>).

REȚELELE DE SOCIALIZARE, JOCURILE ONLINE, LUMILE VIRTUALE ȘI RISCURILE PENTRU COPII



Rețelele sociale sunt spații online unde copiii țin legătura cu familia, cu prietenii și cu oamenii pentru a împărtăși lucrurile pe care le doresc. Cel mai popular este Facebook, unde utilizatorii pot partaja știri, comentarii, imagini și video. Alte rețele sociale populare printre adolescenții din Moldova sunt Twitter, Vkontakte, Odnoklassniki, YouTube pentru videoclipuri și Instagram pentru fotografii.

Pentru a folosi o rețea de socializare, e suficient ca să îți creiezi un cont folosind adresa de email și introducând date ca numele, genul, data de naștere. Pe lângă afișarea informațiilor de profil furnizate de către copil și a intereselor sale, rețelele de socializare permit utilizatorilor săi să posteze statusuri, să se joace jocuri, să vorbească pe chat, să comenteze pe profilurile altor persoane și multe altele.

Copiii își pot posta locația lor fizică ori, pot fi marcați de către prietenii săi într-o locație. Această opțiune ar trebui dezactivată când vorbim despre copii.

Riscul cel mai mare la care sunt expuși copiii atunci când sunt conectați la o rețea de socializare sunt comentariile nedorite atât din partea prietenilor, cât și din partea unor persoane necunoscute. Acestea pot să infiltrează și în viața reală a copiilor și îi afectează creându-le stări de tensiune. Adolescenții care folosesc rețele de socializare creează o amprentă digitală care nu mai poate fi ștearsă, lăsând în spate poze sau comentarii pe care să le regrete mai apoi. Ceea ce poate părea amuzant într-un anumit moment, poate, de asemenea, să afecteze viața personală și profesională mai târziu.

EXPLORAȚI MAI ÎNTÂI SETĂRILE DE SIGURANȚĂ

Majoritatea rețelelor sociale au propriile setări de siguranță și proceduri de raportare. Dacă copilul dvs. crează un nou cont pe o rețea socială, ajutați-l să exploreze aceste setări și instrumente.

Unele dintre cele mai importante includ selectarea opțiunilor potrivite de confidențialitate și securitate și verificarea modului de blocare sau de raportare ale anumitor utilizatori în cazul în care ceva nu merge bine online. (https://web.facebook.com/safety/tools/?_rdc=1&_rdr, <https://help.twitter.com/>, <https://help.instagram.com/196883487377501>).

Înțelegând setările de confidențialitate, numele și poza de profil sunt întotdeauna vizibile public. Acest lucru înseamnă că alți utilizatori pot vedea aceste informații atunci când ajung pe pagina unui anumit utilizator. Informația poate fi făcută accesibilă Tuturor, Prietenilor prietenilor sau Doar prietenilor. De asemenea, se poate limita cine ar putea să vadă poze, comentarii sau alte conținuturi postate de către utilizator. Dacă un adolescent are o pagină pe o rețea de socializare, este important ca părintele să stea alături de ei și împreună să revizuiască setările de siguranță.

SFATURI DESPRE CUM SĂ VORBIM CU ADOLESCENȚII DESPRE REȚELELE SOCIALE

- Vorbiți cu copiii despre controlul asupra propriilor informații. Încurajați-i pe aceștia să fie selectivi cu privire la informațiile pe care le postează. Aplicațiile pe care le folosesc și jocurile în care se joacă pot și ele să fie văzute de către ceilalți.
- Revizuiți setările împreună cu adolescenții și asigurați-vă că sunt setate astfel încât doar prietenii să poată vedea profilul lor.
- Dezactivați serviciile de geo-locăție. Copiii pot, de asemenea, să-și marcheze (tag) și alți prieteni ca fiind prezenți la respectivul loc. Este recomandat ca această opțiune să fie dezactivată în cazul copiilor și tinerilor.
- Discutați cu privire la ceea ce este potrivit să posteze. Nu este permis ca adolescenții să posteze poze în ipostaze discutabile care i-ar putea afecta pe viitor. Totodată, ei trebuie să se gândească bine înainte de a posta statusuri sau comentarii

- Încurajați-i să se întrebe de ce postează un anumit lucru, cine va putea să vadă lucrul respectiv și dacă acest conținut ar putea fi înțeles greșit sau chiar folosit împotriva lor mai târziu.
- Împrieteniți-vă pe Facebook cu copiii mai mici. La această vârstă, copiii nu înțeleg exact anumite concepte și nu știu că ei lasă o “amprentă” digitală. De aceea, e bine să vedeți ceea ce ei postează.
- Întrebați adolescenții dacă sunt de acord să vă fie prieteni pe Facebook. Mulți dintre ei vor fi de acord, dar e bine să nu fiți intruzivi și să nu postați foarte multe comentarii, să vă împrieteniți cu prietenii lor, etc.
- Dacă vreți să evitați situația în care cei mici se retrag din prietenia cu dumneavoastră de pe Facebook, atunci nu le faceți observații cu privire la orice mic lucru. Vorbiți mai mult despre aspecte mai generale și cu adevărat importante.

PROTECȚIA DATELOR CU CARACTER PERSONAL



Cea mai importantă problemă pe care o ridică utilizarea rețelelor sociale o reprezintă protecția datelor cu caracter personal. Respectul pentru viața privată și protecția datelor cu caracter personal sunt două elemente esențiale în societatea contemporană bazată pe utilizarea tehnologiilor moderne de informare și comunicare. Orice informație postată online va rămâne accesibilă, cel mai probabil pentru totdeauna. Copiilor trebuie să li se explice ce informații reprezintă date cu caracter personal, când acestea pot fi sau nu transmise, care sunt situațiile când ele nu vor fi niciodată dezvăluite și ce consecințe există când nu respectăm regulile de protecție a informațiilor confidențiale.

CE ÎNSEAMNĂ DATE CU CARACTER PERSONAL?

<https://www.moldcell.md/rom/news/ce-sunt-datele-caracter-personal-cum-le-protej%C4%83m>

Datele cu caracter personal sunt orice informații ce permite identificarea unui individ.

Date cu caracter personal (categoria obișnuită) se considera:

- | | |
|--|--|
| 1) numele și prenumele; | 18) semnătura; |
| 2) sexul; | 19) datele din actele de stare civilă; |
| 3) data și locul nașterii; | 20) numărul dosarului de pensie; |
| 4) cetățenia; | 21) codul personal de asigurării sociale (CPAS); |
| 5) IDNP; | 22) codul asigurării medicale (CPAM); |
| 6) imaginea; | 23) numărul de telefon/fax; |
| 7) vocea; | 24) numărul de telefon mobil; |
| 8) situația familială; | 25) adresa (domiciliului/reședinței); |
| 9) situația militară; | 26) adresa e-mail; |
| 10) datele de geolocalizare/datele de trafic; | 27) datele genetice; |
| 11) porecla/pseudonimul; | 28) datele biometrice și antropometrice; |
| 12) datele personale ale membrilor de familie; | 29) datele dactiloscopice; |
| 13) datele din permisul de conducere; | 30) profesia și/sau locul de muncă; |
| 14) datele din certificatul de înmatriculare; | 31) formarea profesională – diplome – studii; |
| 15) situația economică și financiară; | 32) obișnuințele/preferințele/comportamentul; |
| 16) datele privind bunurile deținute; | 33) caracteristicile fizice. |
| 17) datele bancare; | |

DE CE DATELE CU CARACTER PERSONAL TREBUIE PROTEJATE?

Într-o lume în care informația capătă o valoare din ce în ce mai mare, datele personale devin o monedă de schimb, mai ales prin intermediul rețelelor de socializare. Iar în grupul țintă al celor interesați de colectarea acestor informații sunt incluși și copiii. Companiile care dețin rețelele de socializare s-au specializat în colectarea de informații, pentru o publicitate mai bine țintită în funcție de particularitățile utilizatorilor. De asemenea, numărul siteurilor piratate (false) e în creștere, creând un pericol serios la adresa securității datelor postate online. Imaginile încărcate pe diferite site-uri sau rețele de socializare pot fi preluate cu ușurință, iar dacă acestea conțin elemente clare de identificare a domiciliului sau programului familiei, situația devine gravă atât pentru copil cât și pentru membrii familiei. Fotografiile compromițătoare se pot transforma în viitor în obstacole la angajare sau vor afecta imaginea publică a tânărului. Nu în ultimul rând, folosirea datelor bancare pentru achiziționarea online de bunuri sau servicii reprezintă un risc la adresa securității financiare a deținătorului cardului. Explicațiile clare și exemplele oferite chiar din experiența lor directă îi pot ajuta să adopte un comportament preventiv pentru o mai bună protecție a datelor și imaginii lor personale.

COMPORTAMENTUL ONLINE AL ADOLESCENȚILOR

Nimeni nu este de acord cu dezvăluirea datelor personale necunoscuților sau expunerea lor publică. Nici copiii nu ar accepta așa ceva. Însă, aflați în fața monitoarelor, mulți dintre adolescenți acceptă cu ușurință furnizarea detaliilor privind identitatea lor sau a familiei pentru a-și crea o adresa de e-mail, pentru participarea la un concurs online sau pentru a intra în posesia unui cadou. De asemenea, adolescenții și tinerii cu conturi pe rețelele de socializare au tendința de a posta o multitudine de informații cu caracter personal.

Pentru oricare dintre situațiile de mai jos, copiii trebuie învățați să ceară consimțământul părinților:

- Dezvăluirea numelui și adresa copilului unei persoane necunoscute, de exemplu, ca parte a termenelor și condițiilor de participare la un concurs;
- Folosirea elementelor de identitate pentru scopuri publicitare;
- Postarea imaginii copilului pe un website public;
- Colectarea de date personale aparținând membrilor familiei sau prietenilor.

[Importanța autoreglementării de către părinți, reprezentanți legali, administratori de instituții preșcolare, școlare a accesului la Internet pentru prevenirea sau limitarea impactului negativ asupra copiilor](#)

Părinții și profesorii trebuie să înțeleagă aceste riscuri pentru a afla la timp când copiii trec prin astfel de experiențe online sau offline. Copiii ai căror părinți sau profesori pun în discuție în mod regulat siguranța pe Internet tind să aibă un comportament mai responsabil când folosesc rețelele sociale sau webcam-urile, ori când transmit mesaje, colectează informații sau postează pe blog-ul sau paginile personale.

Utilizarea frecventă a Internetului însoțită de niveluri mici de competențe este probabil să ducă la experiențe online mai riscante și mai dăunătoare. Nu în mod surprinzător, copiii semnalează niveluri mari de risc atunci când vine vorba de hărțuirea online și vizionarea/primirea de mesaje sexuale, fiind ulterior deranjați și supărați de aceste experiențe. Atunci când vorbim despre experiențele neplăcute, copiii nu cunosc modalitățile prin care se pot proteja: ei vorbesc foarte puțin cu maturii despre experiențele lor dureroase și au tendința de a adopta atitudini pasive atunci când fac față unor astfel de situații, sperând că situația va trece de la sine. De asemenea, experiențele cu care se confruntă cel mai des și care implică risc, hărțuirea și vizionarea/primirea de mesaje cu conținut sexual, trec neobservate de părinții lor.

Atunci când vine vorba de întâlnirea în lumea reală a unor persoane cunoscute online, părinții sunt mai puțin conștienți de întâlnirile pe care le au copiii lor.

Copiii și tinerii sunt utilizatorii activi ai serviciilor noastre. Lucrăm pe cont propriu și împreună cu parteneri experimentați pentru a promova o utilizare mai sigură a internetului în rândul copiilor, tinerilor și părinților lor.

Credem că internetul îmbogățește viața copiilor și le oferă oportunități de a-și îmbunătăți abilitățile digitale, precum și de a socializa, juca și învăța. Cu toate acestea, copiii sunt deosebit de vulnerabili la amenințările online, cum ar fi agresiunea cibernetică și conținutul necorespunzător. Păstrarea siguranței online a copiilor necesită o abordare integrată în întreaga industrie tehnologică și în societate.

Moldcell, împreună cu partenerii săi, promovează **abordări comune** pentru navigarea în condiții de siguranță și utilizarea aplicațiilor, precum și comportamentul respectuos în rândul copiilor și al tinerilor

Aici la Moldcell, ne propunem să ajutăm părinții să echipeze copiii și tinerii cu abilitățile de care au nevoie pentru a rămâne în siguranță online. Astfel, în 2018 am lansat o inițiativă de voluntariat pentru angajați **Internet fără griji**, permițându-le să desfășoare discuții în școli cu privire la modul în care părinții își pot ajuta copiii să navigheze lumea online în condiții de siguranță.

În cadrul sesiunilor **Internet fără griji** ne propunem să diseminăm informații despre cele mai proeminente riscuri, cele mai eficiente metode de control parental și metode de mediere, în același timp făcându-le ușor accesibile și ușor de utilizat.

Proiectul **Internet fără griji**, vizează educația în domeniul noilor tehnologii a copiilor, tinerilor dar și a părinților și profesorilor în calitate de piloni ai dezvoltării armonioase a celor mici.

Experiența acumulată de noi de la părinți, profesori, dar și specialiștii invitați în cadrul seminarelor **Internet fără griji**, ne-au ajutat să ajungem la concluzia că:

- Păstrarea siguranței în mediul online a devenit o obligativitate pentru dezvoltarea optimă a copiilor;
- Internetul poate fi mai degrabă un prieten de bază decât un dușman de temut dacă este folosit responsabil;
- Dezvoltarea Internetului și a noilor tehnologii au schimbat iremediabil viața de zi cu zi a oamenilor, comunicarea, capacitatea de înțelegere a lucrurilor, posibilitățile de dezvoltare și exprimare;
- Cel mai bun lucru pe care îl putem face în momentele în care tehnologia se dezvoltă este de a ne adapta, de a încerca să o înțelegem și să o folosim inteligent pentru a putea profita la maxim de această extraordinară resursă;
- Este momentul să începem să avem grijă de imaginea pe care ne-o creăm în mediul online și să fim conștienți de efectele pe care reputația din spațiul virtual o poate avea asupra noastră pe termen lung.

Vom continua acest proiect și în 2019 pentru a acoperi un număr cât mai mare de părinți și copii din Republica Moldova.

INSTRUMENTELE DISPONIBILE PENTRU AUTOREGLEMENTAREA ACCESULUI LA INTERNET

Utilizarea în siguranță și responsabilă a internetului de către copii depinde în mare măsură de gradul de implicare a părinților, de modul în care aceștia stabilesc un dialog și o comunicare deschisă privind dificultățile întâlnite pe Internet. Copiii au nevoie, în primul rând, de îndrumare și confirmare din partea părinților că activitățile lor online sunt sigure și utile în educația lor. O măsură complementară pentru protejarea copiilor în timpul utilizării Internetului și controlul activității acestora o reprezintă programele de filtrare a conținutului web și de control parental.

Există o mai multe instrumente de control pentru părinți și alte instrumente online pentru a vă ajuta copilul să aibă o experiență online mai sigură și mai personală, multe dintre acestea fiind gratuite și ușor de configurat. (<https://www.moldcell.md/rom/private>).

S-ar putea să aveți deja un instrument de control parental pentru părinți pe computerul copilului dvs., sau smartphone-ul și tableta, dar țineți minte că controalele și instrumentele nu sunt întotdeauna eficiente 100%.

Programele de filtrare a conținutului web și de control parental sunt programe complexe pentru controlul accesului copiilor la calculator sau Internet, în scopul diminuării riscurilor online. Aceste programe se găsesc contra cost sau gratuit și pot fi instalate fie pe calculatorul copiilor, fie pe dispozitive mobile (telefon, tabletă, iPad etc). Se recomandă în mod special setarea unor profile (users) separate pentru copii și utilizarea acestor programe atunci când părinții nu pot fi în permanență în apropierea copiilor în timp ce aceștia folosesc Internetul. Principalele funcții ale acestor soluții software sunt (atât pentru telefoane și dispozitive mobile, cât și calculatoare):

- Filtrarea conținutului web pe baza unor liste de adrese sau cuvinte restricționate:
 - blochează accesul la anumite site-uri pe baza unei liste predefinite de adrese interzise.
 - analizează conținutul și blochează accesul pe anumite pagini pe baza unei liste predefinite de cuvinte interzise
 - permite accesul doar la anumite site-uri pe baza unei liste predefinite de adrese acceptate.
- Controlul utilizării și accesului la Internet și calculator / dispozitive mobile la programe și fișiere:
 - limitează timpul petrecut de copii la calculator și/sau Internet, prin stabilirea unor intervale orare în care copilul poate avea acces la acestea;
 - limitează tipurile de programe și fișiere care pot fi descărcate și instalate pe calculator;
 - blochează accesul la informațiile personale sau de lucru stocate pe calculator (de exemple, documente, fotografii personale) prin blocarea accesului la anumite fișiere sau partiții de disc;
 - limitează sau blochează utilizarea unor programe de către copii (messenger, partajare de fișiere, programe utilizate de către părinți).
 - limitează sau blochează accesul la setările calculatorului.
- Monitorizarea utilizării calculatorului / dispozitivului mobil și a Internetului.
 - întocmește lista cu site-urile pe care le-a accesat copilul, astfel că aceasta poate fi verificată de părinți.

- întocmește rapoarte cu pagini vizitate, programe utilizate, timp alocat, fișiere accesate/create/șterse sau chiar imagini de tip printscreen cu activitatea copiilor la calculator sau Internet.
- trimite pe email-ul părinților rapoarte periodice cu activitatea copiilor la calculator.

Pentru a asigura navigarea cât mai sigură a copiilor în mediul on-line, am pus la dispoziția părinților soluția Kaspersky Safe Kids (<https://www.moldcell.md/rom/private/servicii/safe-kids>):

- setezi aplicațiile permise copilului spre utilizare
- stabilești intervalele de timp, între care copilul poate utiliza dispozitivele mobile
- monitorizezi activitatea copilului tău pe câteva rețele de socializare odată (Facebook și VK)
- setezi restricții pentru anumite site-uri sau limitezi accesul temporar la acestea
- primești notificări, în momentul în care se detectează careva acțiuni suspicioase
- vezi localizarea exactă a copilului tău/dispozitivului său mobil, pe hartă
- monitorizezi apelurile telefonice și mesajele SMS primite și expediate pe/de pe numărul copilului tău (lista numerelor de telefon)
- restricționezi apelurile și mesajele SMS de la numere nepermise și ești notificat despre acestea
- primești rapoarte privind activitatea copilului tău pe Internet.

Configurare control parental Windows

Microsoft oferă controale pentru părinți pentru a ajuta copiii să rămână în siguranță când folosesc computerul de familie. Configurați aceste controale pentru a limita tipurile de aplicații pe care le pot utiliza, ce site-uri web le este permis să viziteze și cât timp pot cheltui pe computer și pe alte dispozitive bazate pe Windows. După ce sunt configurate controalele părintești, puteți accesa rapoarte detaliate despre activitatea lor.

Controlul parental, așa cum este prezentat aici, se aplică numai atunci când copilul se conectează la un dispozitiv Windows utilizând propriul Cont Microsoft. Aceste setări nu vor împiedica ceea ce fac pe computerele prietenilor, pe computerele școlare sau pe dispozitivele Apple sau Android sau când accesează un computer în contul altcuiva (chiar și în contul dvs.).

Activați controlul parental Windows 10

Pentru a utiliza cele mai recente funcții de control parental Windows și caracteristicile Microsoft Family Safety, atât dvs., cât și copilul dvs. aveți nevoie de un cont Microsoft (nu unul local). Deși puteți obține un cont Microsoft pentru copilul dvs. înainte de a configura controalele parentale disponibile în Windows 10, este mai simplu să creați contul în timpul procesului de configurare. Orice ați decide, urmați acești pași pentru a începe:

- 01) Faceți clic pe Start> Setări (Settings). (Pictograma Setări arată ca o curea.)
- 02) În Setări Windows, faceți clic pe Conturi (Accounts).
- 03) În panoul din stânga, faceți clic pe Familie și alte persoane (Family & Other People).
- 04) Faceți clic pe Adăugați un membru de familie (Add a Family Member).
- 05) Faceți clic pe Adăugați un copil (Add a Child) și apoi pe Persoana pe care doresc să o adăugați nu are o adresă de e-mail (The Person I Want To Add Doesn't Have An Email Address). (Dacă au o adresă de e-mail, tastează-o, apoi treceți la pasul 6.)

- 06) În caseta de dialog Creare cont (Let's Create An Account), dați informațiile necesare, inclusiv contul de e-mail, parola, țara și data nașterii.
- 07) Faceți clic pe Următorul (Next). Faceți clic pe Confirmare dacă vi se solicită.
- 08) Citiți informațiile oferite (ceea ce vedeți aici depinde de ceea ce ați selectat în pasul 5) și faceți clic pe Închidere (Close).

Dacă ați obținut un cont Microsoft pentru copilul dvs. în timpul procesului de mai sus, veți observa că copilul a fost adăugat pe lista membrilor de familie din Setările Windows (Windows Settings) și că statutul este Copil (Child). Controalele parentale sunt deja activate utilizând cele mai comune setări, iar contul este gata de utilizare. Conectați-vă copilul la cont în timp ce sunteți conectat (ă) la internet pentru a finaliza procesul.

Dacă introduceți un cont Microsoft existent în timpul procesului de mai sus, vi se va solicita să vă conectați la acel cont și să urmați instrucțiunile din e-mailul de invitație. În acest caz, statutul contului va indica Copil, În așteptare (Child, Pending). Copilul va trebui să se conecteze la internet pentru a finaliza procesul de configurare. De asemenea, este posibil să vi se aplice manual setările de siguranță pentru familie, dar acest lucru depinde de mai mulți factori. Citiți următoarea secțiune pentru a afla cum să determinați dacă controalele sunt setate sau nu.

Găsiți, schimbați, activați sau dezactivați controlul parental (Windows 10)

Există șanse egale că comenzile implicite pentru siguranța familiei Windows (Windows Family Safety controls) sunt deja activate pentru contul copilului dvs., însă este o bună practică să verificați acest lucru și să vedeți dacă acesta corespunde nevoilor dvs. Pentru a examina setările, a le configura, modifica, activa sau dezactiva sau pentru a activa raportarea pentru un cont Microsoft:

- 01) Faceți clic pe Start > Setări (Settings) > Conturi (Accounts) > Familie și alte persoane (Family & Other People), apoi faceți clic pe Gestionați setările familiei online (Manage Family Settings Online).
- 02) Conectați-vă dacă vi se solicită, apoi localizați contul copil din lista de conturi inclusă împreună cu familia.
- 03) Activați Setarea limitelor de timp în care copilul meu poate utiliza dispozitivele (Set Limits For When My Child Can Use Devices) pentru a modifica setările implicite ale ecranului utilizând listele derulante și calendarele zilnice. Dezactivați această setare dacă doriți.
- 04) În panoul din stânga, faceți clic pe Navigare Web (Web Browsing).
- 05) Porniți Blocare site-uri neadecvate (Block Inappropriate Websites). Citiți ce tipuri de conținut sunt blocate și asigurați-vă că opțiunea Căutarea sigură (Safe Search) este activată.
- 06) În panoul din stânga, faceți clic pe Aplicații, Jocuri și Media (Apps, Games, & Media). Asigurați-vă că Blocare Aplicații neadecvate și Jocuri (Block Inappropriate Apps And Games) este deja activată.
- 07) Faceți clic pe Raportarea activităților (Activity Reporting). Faceți clic pe Activare raportare activitate (Turn On Activity Reporting) pentru a obține rapoarte săptămânale despre activitățile copilului dvs. în timp ce sunteți online. Rețineți că copilul trebuie să utilizeze Edge sau Internet Explorer și că puteți bloca alte browsere.
- 08) Continuați să explorați alte setări după cum doriți.

Windows 8 și 8.1 Control parental

Pentru a activa controlul parental în Windows 8 și 8.1, trebuie mai întâi să creați un cont pentru copilul dvs. Faceți acest lucru în Setări PC (Settings). Apoi, din Panoul de control (Control Panel), configurați setările dorite pentru contul copil.

Pentru a crea un cont copil în Windows 8 sau 8.1:

- 01) Din tastatură, țineți apăsată tasta Windows și apăsați C.
- 02) Faceți clic pe Modificare setări PC (Change PC Settings).
- 03) Faceți clic pe Conturi (Accounts), faceți clic pe Alte conturi (Other Accounts), faceți clic pe Adăugați un cont (Add An Account).
- 04) Faceți clic pe Adăugați un cont copil (A Child's Account).
- 05) Urmăriți instrucțiunile pentru a finaliza procesul, optați pentru crearea unui cont Microsoft (Microsoft Account) peste un cont local, dacă este posibil.

Pentru a configura Controlul părintesc:

- 01) Deschideți panoul de control (Control panel). Puteți să îl căutați din ecranul de pornire sau din spațiul de lucru.
- 02) Faceți clic pe Conturi de utilizator și siguranța familiei (User Accounts And Family Safety), apoi faceți clic pe
- 03) Faceți clic pe contul copilului.
- 04) Sub Control parental (Parental Controls), faceți clic pe Aplicați setările curente (Enforce Current Settings).
- 05) În secțiunea Raportarea activităților (Activity Reporting), faceți clic pe Colectați informații despre utilizarea PC-ului (Collect Information About PC Usage).
- 06) Faceți clic pe linkurile furnizate pentru următoarele opțiuni și configurați după cum doriți:
 - Filtrarea web (Web Filtering) pentru a bloca anumite site-uri web și pentru a împiedica descărcările;
 - Limitări de timp (Time Limits) pentru a alege când și în ce zile copilul dvs. poate accesa PC-ul;
 - Magazin Windows (Windows Store) și **Restricții de joc** (*Game Restrictions*) pentru a seta limite de vârstă, titlul și limită de rating pentru aplicațiile pe care copilul dvs. le poate utiliza;
 - Restricții de aplicații (App Restrictions) pentru a seta aplicațiile pe care copilul dvs. le poate utiliza.
- 07) Veți primi un e-mail care conține informații despre pagina de conectare la Microsoft Family Safety și ce este disponibil acolo. Dacă utilizați un Cont Microsoft pentru copilul dvs., veți putea să vizualizați rapoartele de activitate și să efectuați modificări online, de pe orice computer.

CONFIGURAREA CONTROL PARENTAL PENTRU WINDOWS 7

Configurați controlul parental în Windows 7 din Panoul de control (Control panel), într-un mod similar cu cel prezentat mai sus pentru Windows 8 și 8.1. Va trebui să creați un cont copil pentru copil în Panoul de control (Control panel) > Conturi utilizator (User Accounts) > Dați altor utilizatori acces la acest computer (Give Other Users Access To This Computer). Lucrați prin procesul așa cum vi se solicită.

- 01) Faceți clic pe butonul Start și tastați Control parental în fereastra de căutare (Parental Controls in the search window).
- 02) Faceți clic pe Control parental (Parental Controls) în rezultate.
- 03) Faceți clic pe contul copil.

- 04) Dacă vi se solicită, creați parole pentru orice conturi de **Administrator** (*Administrator accounts*).
- 05) În **Control parental** (*Parental controls*), selectați **Aplicați setările curente** (*Enforce Current Settings*).
- 06) Faceți clic pe următoarele linkuri și configurați setările după caz, apoi faceți clic pe **Închidere: Limite de timp, Jocuri și Permiteți și blocați anumite programe** (*Close: Time Limits, Games, and Allow And Block Specific Programs*).

INSTITUȚIILE ABILITATE UNDE SE POT RAPORTA ABUZURILE DIN MEDIUL ONLINE, CONȚINUTURILE CONSIDERATE ILEGALE SAU DĂUNĂTOARE COPIILOR

Instituțiile abilitate unde se pot raporta abuzurile din mediul online, conținuturile considerate ilegale sau dăunătoare copiilor.

Dacă, atunci când stai pe net, te simți agresat, ai îndoieli, întrebări, sau vrei doar să vorbești cu un specialist, contactează <https://telefonulcopilului.md> sau agenții noștri la numărul 444 (apel gratuit) care te vor ghida.

Alte surse de unde poți afla mai multe despre întrebările care te frământă:

<https://siguronline.md>; <https://onlinesafety.info>; <https://contentfiltering.info>; www.safeinternet.org;
<https://www.soros.md/publication>; www.itu.int/cop, <https://siguronline.md/rom/copii>
<http://lastrada.md/>