Confederaţia Caritas România

Stadiul aprobare:	Aprobat		
Pregătit de:	Thomas Hackl	Data:	25.11.2021
Aprobat de:	Cons. Dir.	Data:	02.12.2021

Politică de salvgardare a copiilor în mediul online

Ghid de aplicare a procedurilor de salvgardare

Cuprins:

Acest document a fost elaborat în cadrul proiectului „În lumea virtuală - Educație inteligentă și sigură", finanțat de Secours Catholique – Caritas France.

La elaborarea documentului au contribuit:

Adela Popa-Ghițulescu – Caritas Eparhial Oradea
Florentina Ciobanu – Caritas Eparhial Cluj
Ioana Găvrilaș – Confederația Caritas România
Janos Boros – Organizația Caritas a Diecezei Satu Mare
Margareta Ferenț – Centrul Diecezan Caritas Iași
Ramona Marichici – Federația Caritas Timișoara
Thomas Hackl – Confederația Caritas România
Valentina Balint – Federația Caritas Timișoara

1. Introducere

Mediul online joacă un rol din ce în ce mai mare în viața copiilor, având implicații importante în educația lor, dar și în modul în care își petrec timpul liber. Pandemia de Covid-19 a accelerat procesul de digitalizare a societății odată cu închiderea școlilor, predarea și învățarea desfășurându-se în mare măsură în mediul online. Din cauza restricțiilor de contact direct, comunicarea prin aplicații online și prin social media a căpătat o importanță nemaiîntâlnită. Noile forme de muncă în „home office" au contribuit de asemenea la digitalizarea societății și chiar și în relațiile cetățenilor cu autoritățile de stat, internetul începe să aibă un rol esențial.

Astfel și copiii din medii vulnerabile care până nu de mult au avut un acces foarte limitat la mediul online se regăsesc într-o lume virtuală pentru care nu au fost pregătiți. De multe ori, centrele de zi și centrele afterschool Caritas au facilitat accesul copiilor în mediul online și au oferit asistență pentru a face față noilor cerințe.

Digitalizarea societății, în special a școlii, aduce multe oportunități, dar în același timp copiii, mai ales cei care provin din medii care până nu de mult nu au avut acces la lumea virtuală, sunt expuși și multor riscuri.

Politica de salvgardare în mediul online are ca scop crearea de condiții sigure în centrele Caritas, în care copiii au șansa să participe la lumea virtuală, fiind protejați de riscuri și își pot dezvolta capacitatea de a face față acestor riscuri nu numai la centru Caritas, ci și în propria lor viață.

2. Declarația de salvgardare a Caritas în România

Mediul online are un rol important în viața copiilor și este strâns legat de educație și învățare, comunicare și petrecerea timpului liber. Caritas România conștientizează importanța participării copiilor din mediile defavorizate la activități în „lumea virtuală" și a valorificării oportunităților oferite copiilor în acest mediu dar, cunoaște și este preocupată să prevină riscurile la care sunt expuși copiii în mediul online.

În politica sa de salvgardare care are ca bază politica de salvgardare Caritas Internationalis, Confederația Caritas România declară:

„Caritas recunoaște dreptul copiilor și al adulților vulnerabili la protecție, indiferent de sex, rasă, cultură și dizabilitate. ... Caritas se angajează să creeze și să mențină un mediu care promovează valorile sale fundamentale și previne abuzul și exploatarea tuturor oamenilor."

În acest sens, Caritas România și organizațiile membre se angajează să creeze, în centrele proprii, condițiile necesare pentru a folosi resursele online în siguranță și pentru a participa la activitățile de învățare și de petrecerea timpului liber în mediul virtual în mod responsabil.

Caritas se implică în mod activ în dezvoltarea competențelor digitale ale copiilor și în creșterea conștientizării riscurilor din mediu online.

De asemenea, Caritas prin centrele pentru copii, oferă sprijin concret pentru copiii care au fost victimele abuzurilor în mediul virtual și se angajează să intervină prompt când copiii care se află în

grija organizației, sunt în pericol iminent să devină victimele unui abuz în mediul online și să anunțe, dacă este cazul, autoritățile de stat competente.

3. Termeni utilizați și analiza riscurilor

Riscurile pentru copii (dar și pentru adulți) în mediul online sunt multiple și țin de mai multe aspecte:

Conținuturi nepotrivite pentru copii

Conținutul nepotrivit se referă la orice material scris/audio/vizual găsit pe internet care are o influență negativă asupra dezvoltării copilului. Aceste conținuturi ar putea tenta minorul să adopte un comportament ilegal sau periculos sau îl pot afecta emoțional.

Categorii de conținut nepotrivit:

- Site-uri care încurajează vandalismul, criminalitatea, terorismul, rasismul, sexismul, alimentația nesănătoasă, și chiar suicidul;
- Materiale pornografice, limbaj licențios și vulgarități;
- Imagini, videoclipuri sau jocuri care demonstrează imagini de violență sau cruzime față de alte persoane sau animale;
- Site-uri cu jocuri de noroc;

Pe măsură ce copilul devine mai activ online, posibilitatea și probabilitatea ca el sa vadă ceva necorespunzător vârstei sale depinde și de ceea ce face online.

Accesarea conținutului nepotrivit este posibilă pe orice dispozitiv conectat la internet. Copilul poate întâlni materiale necorespunzătoare pe site-uri web, aplicații, link-uri trimise de prieteni sau în timp ce discută cu alții online.

Transmiterea, pe telefon, de imagini sau mesaje cu caracter sexual constituie o practică frecventă în a cărei capcană cad numeroși minori.

Fake news și manipulare

Știrile false și manipulatoare au scopul de a distorsiona percepția auditoriului sau crearea unui nou curent de opinie cu intenția de a dezinforma sau de a crea confuzie și a destabiliza sentimentul de securitate (colectivă, națională). De multe ori prin știri false se urmărește deteriorarea reputației unei instituții, entități sau persoane, precum și câștiguri financiare sau politice.

Una dintre cele mai importante caracteristici ale știrilor false este faptul că ele caută să stârnească o reacție emoțională puternică, caută să trezească emoții precum teamă, stres, neîncredere, dezgust, furie, panică. Expunerea excesivă la știri false, cuplată mai ales cu o lipsa de comunicare în familie, poate duce cu rapiditate la adâncirea unor stări de anxietate sau chiar depresie.

Infectarea dispozitivelor cu programe dăunătoare (malware)

Există mai multe tipuri de programe dăunătoare cu diferite moduri de funcționare și distribuire: viruși informatici, vierme informatic, cai troiani. Aceste programe sunt instalate neintenționat și de cele mai multe ori neobservat pe calculatoare și alte dispozitive și au diferite scopuri:

- Spionarea datelor salvate pe calculator (inclusiv parole și date personale)
- Urmărirea utilizatorului în scopuri de marketing
- Distrugerea datelor sau a dispozitivelor (sau șantaj prin criptarea datelor)
- Folosirea dispozitivului pentru alte scopuri (trimitere de spam, atacarea altor sisteme informatice, etc.)

Programele dăunătoare ajung pe dispozitive informatice pe mai multe căi:

- Drive-by downloads - prin simpla vizitare a unei pagini web programele dăunătoare sunt descărcate și instalate pe calculator.
- Infectare prin deschiderea fișierelor trimise prin email, link-uri, fișierelor luate de pe platforme de distribuirea fișierelor (video, muzică, jocuri)
- Programe dăunătoare care sunt atașate altor programe distribuite (de multe ori în mod gratuit) pe internet

Dezvăluirea informațiilor personale și contactarea de către persoane necunoscute și rău-intenționate

Informațiile personale și confidențialitatea acestora reprezintă o temă destul de neglijată de către adulți și mai ales de către copii care nu au modele de practici pozitive în păstrarea confidențialității datelor cu caracter personal, ce nu trebuie să spui, să postezi sau să arăți pe platformele online.

Identitate falsă: poză, vârstă, etc.

Unde și cum sunt contactați copiii de persoane necunoscute?

- Platforme de social media - prin comentarii la postările publicate
- Prin programe de messenger (facebook, messenger, whatsapp, etc.)
- Chatroom din jocurile online
- Email

Două situații diferite:

- Partajarea informațiilor personale în mod voluntar și din propria inițiativă: publicate în social media ca și conținut public, divulgarea parolelor pentru conturi de social media și de email, trimiterea de poze și filmări video cu conținut confidențial/intim, etc.
- Spargerea conturilor și furtul datelor de către persoane neautorizate

Riscurile:

- Să divulge date cu caracter personal(date, informații, imagini) persoanelor adulte ce au interese ascunse.
- Să devină victimele cyberbullying-ului și să nu știe cum să facă față sau cum să reacționeze.

- Să fie răspândite informații, minciuni sau postări cu fotografii despre copilul vizat.
- Să primească mesaje jignitoare/amenințătoare(conotație sexuală/pedofilă).
- Să-i fie furată identitatea și să fie realizat un cont fals de pe care să se trimită mesaje către alte persoane sau obținerea accesului la conturile personale ale copilului/tânărului.
- Intrare în contact direct cu copilul/tânărul în „lumea reală" cu scopuri ilegitime (exploatare, pedofilie, etc.)
- Cyberbullying și șantajarea persoanei.

Cyberbullying

Cyberbullying-ului se referă la „diferite forme de abuz psihologic comis prin acte de hărțuire transmise prin tehnologiile de informare și comunicare, cum ar fi internetul. Acestea sunt acte de violență și se fac în scopul amenințării, intimidării sau insultării victimelor. Ele au un caracter repetitiv, putând fi comise atât de către indivizi cât și de grupuri de persoane.

Cyberbullying-ul este un fenomen complex, având mai multe forme de manifestare:

- Bârfa sau comentariile denigrante – presupune emiterea în mediul online a unor declarații speculative, ce pot denigra o anumită persoană sau instigă alte persoane în a adopta un comportament agresiv;
- Excluderea din grupuri sau activități online a anumitor persoane, din cauza faptului că nu este considerată suficient de bună pentru a face parte din același grup;
- Hărțuirea si urmărirea online – luarea în batjocură constantă și repetitivă a unui minor, care poate afecta integritatea psihică a acestuia;
- Insistența abuzivă și instigarea – postări sau trimiteri permanente de mesaje către anumite persoane; provocarea unor persoane să acționeze agresiv;
- Profiluri false – profiluri create de către agresori pe internet, care împrumută identitatea altor persoane, spre a facilita comunicarea cu victimele lor;
- Dezvăluirile – folosirea de trucuri pentru a obține informațiile personale ale victimei, pe care agresorul urmează sa le facă publice;
- Sabotarea și distribuirea de materiale pornografice minorilor utilizând mijloace electronice de comunicare.
- Înregistrarea video a atacurilor – presupune ca agresorul să filmeze victima în timpul atacului și să distribuie clipul video altor persoane, pentru a-l vizualiza și comenta, în acest fel sporind gradul de umilință la care este supusă victima.

Dependența de internet

Dependența de internet este definită prin preocupări excesive pentru mediul on-line, dorința imperioasă și comportamente de utilizare a internetului, toate acestea conducând la disfuncții în plan social, profesional, școlar sau familial, ori la disconfort semnificativ pentru persoana în cauză.

Efecte ale dependenței de internet:

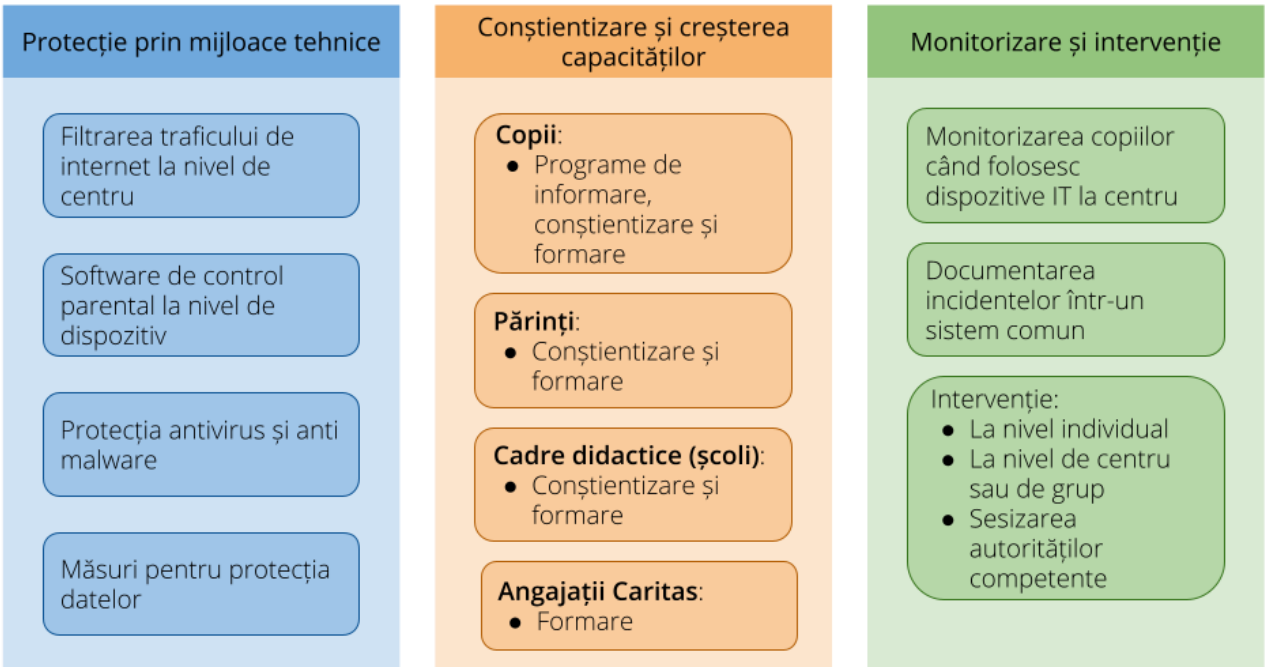
- Izolare socială. Persoanele care dezvoltă dependență de Internet tind să se izoleze de ceilalți, cu un impact negativ asupra relațiilor personale.
- Neîncrederea și lipsa onestității – aceștia tind să ascundă timpul real petrecut online și nu mai au încredere în ceilalți.
- Incapacitatea sau dificultatea de a interacționa cu alte persoane în viața reală.
- Stimă de sine scăzută, cauzată de lipsa interacțiunilor sociale.
- Scăderea rezultatelor la învățătură, probleme comportamentale
- Pierderea plăcerii de a desfășura activități în viața reală, cu oameni reali.

4. Proceduri și intervenții

Amenințările în mediul online pentru copii necesită o abordare complexă și integrată care ia în calcul și aspectele tehnice, dar și cele ce țin de pregătirea și comportamentul copiilor și a persoanelor responsabile pentru acești copii.

Pentru a crește siguranța copiilor în timp ce folosesc dispozitive conectate la internet, conceptul de siguranță Caritas prevede intervenții pe trei planuri:

- Asigurarea condițiilor tehnice pentru folosirea internetului în condiții sigure
- Pregătirea și conștientizarea persoanelor implicate
- Monitorizarea copiilor și intervenție în situații de risc



5. Standarde minime

Caritas implementează un set de standarde minime pentru a proteja copiii beneficiari din centrele organizației. Fiecare standard cuprinde o descriere a situației „sub-standard", adică care nu corespunde cerințelor, indicatori pentru a atinge standardul minim și bune practici care depășesc cerințele standardului și contribuie la o și mai mare siguranță a copiilor.

Lista standardelor:

Protecție prin mijloace tehnice	1.1.	La centrul Caritas, copiii au acces la internet în condiții tehnice de siguranță
	1.2.	Toate dispozitivele din centrele Caritas sunt protejate de viruși și alte forme de malware.
	1.3.	Datele salvate pe dispozitivele centrului (datele salvate de copii, date despre beneficiari, datele angajaților) sunt protejate de accesarea de către persoane neautorizate.
Conștientizare și creșterea capacităților	2.1.	Copiii cunosc principalele riscuri pe internet și știu cum să se protejeze de aceste pericole.
	2.2.	Părinții copiilor cunosc principalele riscuri pe internet și au capacitatea de a-și monitoriza copiii și de a interveni în situații suspecte.
	2.3.	Specialiștii din centre (pedagogi, psihologi, asistenți sociali) au capacitatea de a proteja copiii beneficiari ai centrului de riscurile din mediul online.
Monitorizare și intervenție	3.1.	Copiii sunt monitorizați în timp ce folosesc dispozitive IT în centrul Caritas.
	3.2.	Incidentele în mediul online în care sunt implicați copiii sunt documentate, discutate în echipă și informațiile relevante sunt comunicate către alte centre Caritas.
	3.3.	În cazul unui incident sau abuz asupra unui copil în mediul online, echipa centrului intervine pe plan individual și în grup. Dacă este cazul, sunt implicate și autoritățile competente.
Implementare a politicilor	4.1.	În fiecare centru Caritas în care copiii beneficiari au acces la echipamente IT și în mediul online, există un responsabil (focal point) pentru siguranța copiilor în mediul online.
	4.2.	În fiecare centru Caritas în care copiii beneficiari au acces la echipamente IT și în mediul online, există un plan de siguranță online adaptat la situația concretă a centrului.

Descrierea detaliată a standardelor

Protecție prin mijloace tehnice

Standard 1.1:	La centrul Caritas copiii au acces la internet în condiții tehnice de siguranță
Criterii	
Sub-standard	La centrul Caritas accesul copiilor la internet este nerestricționat și copiii nu sunt monitorizați când accesează internetul.
Minim	• Copiii au acces la internet într-un mediu asigurat în care accesul la pagini și servicii nepotrivite este restricționat prin măsurile tehnice (software de control parental, filtre de content, conturi pentru copii). • Copiii nu au acces la servicii de filesharing (pentru download de filme și programe piratate)
Bună practică 1	Există o listă de situri și servicii care pot fi accesate. Dacă un copil dorește să acceseze un site sau un serviciu ne-inclus în listă, este nevoie de aprobarea (și adăugarea în listă) responsabilului din centru.
Bună practică 2	Restricțiile de acces sunt aplicate nu numai pe dispozitivele din dotarea centrelor, dar și pe dispozitivele copiilor conectate prin rețeaua centrului.

Note de ghidare:

În funcție de dispozitive (și sisteme de operare) și de structura rețelei din centru există mai multe soluții tehnice pentru a restricționa și monitoriza activitatea online:

- Conturile pentru copii și sistemul de control parental integrat în sistemul de operare Windows 10
- Software de control parental: O variantă este Kaspersky Safe Kids (https://www.kaspersky.ro/safe-kids), disponibil în limba română și pentru sisteme de operare Windows, Android, iOS. Există o variantă gratuită.
- Filtre de conținut pe nivel de router: Pe aproape toate routerele pot fi definite filtre de conținut.
- Filtrarea conținutului prin redirecționarea traficului de internet prin serviciul opendns.com

Ultimele doua variante asigură și o filtrare a traficului de internet de pe dispozitivele copiilor conectate prin Wifi-ul centrului.

Standard 1.2:	Toate dispozitivele din centrul Caritas sunt protejate de viruși și alte forme de malware.
Criterii	
Sub-standard	• Nu există restricții la instalare de software

	● Accesul la platforme cu conținut dăunător și ilegal este posibil ● Nu există protecție antivirus actualizată
Minim	● Instalarea de programe și aplicații este posibilă numai pentru persoane autorizate ● Pe toate dispozitivele cu sistemul de operare Windows este instalat un program antivirus actualizat. ● Accesul la platforme de download cu conținut periculos sau ilegal este blocat
Bună practică 1	Se face o scanare completă regulată cu un program antivirus măcar o dată pe lună.
Bună practică 2	Se aplică măsuri de sugiranță la folosirea stick-urilor USB
Bună practică 3	Există o singură persoană în centru care are drepturile de administrator la toate calculatoarele și alte device-uri și care are dreptul de a instala aplicații.

Note de ghidare:

- Folosirea conturilor de copii din sistemul Windows 10 blochează în mod automat posibilitatea de a instala programe și aplicații. Este nevoie de parola administratorului pentru a debloca instalarea.
- Dispozitivele cu sistemul Android pot fi protejate prin aplicații de control parental (https://www.kaspersky.ro/safe-kids) și prin activarea modului de control parental.
- Se evită conectarea la calculator sau laptop a stick-urilor USB necunoscute sau străine. Stick-urile vor fi criptate și protejate cu un program de siguranță.

Standard 1.3:	Datele salvate pe dispozitivele centrului (datele salvate de copii, date despre beneficiari, datele angajaților) sunt protejate de accesarea de către persoanele neautorizate.
Criterii	
Sub-standard	● Există un singur cont de utilizator pe fiecare dispozitiv ● Toate datele salvate pe un dispozitiv sunt accesibile pentru toți utilizatorii
Minim	● Fiecare angajat folosește un cont propriu de acces pe calculator ● Datele personale ale beneficiarilor sunt salvate într-un loc asigurat cu drepturile de acces clar definite ● Copiii folosesc un cont special de acces pentru copii
Bună practică 1	Există o abordare sistematică de salvare și accesare a datelor
Bună practică 2	Fiecare copil are un cont propriu de acces la calculatoare
Bună practică 3	Datele sensibile (în special datele personale ale beneficiarilor și angajaților) sunt criptate și asigurate cu parolă

Bună practică 4	Există un regulament pentru partajarea datelor prin metode de transmitere electronică și pentru salvarea datelor pe medii de stocare externe (stick usb, etc.)

Conștientizare și creșterea capacităților

Standard 2.1.	Copiii cunosc principalele riscuri pe internet și știu cum să se protejeze de aceste pericole.
Criterii	
Sub-standard	Temele de siguranță pe internet nu sunt abordate sau sunt prezentate într-un mod ad-hoc
Minim	● Toți copiii beneficiari participă la un curs standard despre siguranța pe internet, adaptat vârstei lor ● Copiii se adresează angajaților centrului când se confruntă cu situații suspecte sau de risc în mediul online
Bună practică 1	Organizarea de întâlniri regulate (minim o dată pe semestru) de informare și conștientizare a riscurilor, dar mai ales a metodelor de evitare și atenuare a acestora.
Bună practică 2	Organizarea de întâlniri practice cu beneficiarii pentru a învăța cum să-și gestioneze concret și corect conturilor personale în mediul online.
Bună practică 3	Copiii învață singuri despre pericole în mediul online folosind aplicația pregătită de CCR
Bună practică 4	Copiii au acces la alte surse de informare despre pericole în mediul online (cărți, pagini internet dedicate, etc.)

Note de ghidare:

Cursul pentru copii abordează cel puțin următoarele subiecte:

a) Riscurile:
   - Furtul și folosirea informațiilor personale
   - Virusarea dispozitivelor
   - Contactare de persoane necunoscute
   - Cyberbullying, amenințări, șantaj
   - Conținut nepotrivit și deranjant
   - Dependența de internet

b) Metode de protecție referitoare la:
   - Partajarea informațiilor (social media, mesaje, etc.)
   - Contactarea de către persoane necunoscute
   - Siguranța pe social media și platforme online
   - Siguranța dispozitivelor

- Verificarea informațiilor
- Dependența

Standard 2.2.	Părinții copiilor cunosc principalele riscuri pe internet și au capacitatea de a monitoriza copiii și de a interveni în situații suspecte.
Criterii	
Sub-standard	• Părinții copiilor nu sunt văzuți ca parteneri pentru creșterea siguranței copiilor în mediul online
Minim	• Temele de siguranță în mediul online sunt abordate în ședințe cu părinții • Părinții au posibilitatea de a participa la un workshop despre siguranța pe internet și monitorizarea copiilor • Părinții au acces la filme scurte care le explică aspecte de siguranță pe internet
Bună practică 1	Centrele Caritas dispun de un ghid pentru părinți și copii care sa îi ajute să recunoască fenomenul și să îi îndrume în cazul în care copiii sunt victime ale cyberbullying-ului.
Bună practică 2	Părinții au posibilitatea să apeleze la un angajat al centrului Caritas pentru consiliere în probleme legate de siguranța copiilor în mediul virtual.
Bună practică 3	Părinții recunosc importanța tematicii de siguranța a copiilor în mediul online si aplica concret masurile de protecție/monitorizare.
Bună practică 4	Pe dispozitivele personale ale copiilor sunt instalate aplicații de acord parental.

Note de ghidare:

Prin întâlnirile, cursuri, filmulețe și ghiduri, părinții sunt încurajați de a monitoriza activitatea online a copiilor:

- crearea conturilor pentru copii pe dispozitivele folosite de aceștia;
- acces limitat pentru copii pe dispozitive (realizarea unui program/interval orar în care aceștia să aibă acces la internet; de preferat în intervalul în care sunt și părinții acasă);
- folosirea aplicațiilor de acord parental

Standard 2.3.	Specialiștii din centre (pedagogi, psihologi, asistenți social) au capacitatea de a proteja copiii beneficiari ai centrului ,de riscurile din mediul online.
Criterii	
Sub-standard	• Specialiștii din centre nu au capacitatea de a proteja copiii beneficiari ai centrului de riscurile din mediul online pentru că de cele mai multe ori

	nici ei nu le cunosc și nu sunt conștienți de acestea.
Minim	● Specialiștii centrelor au cunoștințe minime în utilizarea calculatoarelor și a altor dispozitive online ● Specialiștii centrelor participă la un curs despre siguranța pe internet și despre politica Caritas de salvgardare în mediul online ● Specialiștii centrelor își actualizează cunoștințele despre siguranța online în mod regulat
Bună practică 1	Cel putin un angajat al centrului știe să ghideze copiii în adoptarea setărilor de privacy, instalare de software de protecție, blocarea conturilor, raportarea cazurilor de hărțuire, etc.
Bună practică 2	Specialiștii din centre pot proteja copiii prin identificarea riscului și găsirea unei soluții imediate
Bună practică 3	Pedagogii sunt încrezatori în forțele proprii și transmit copiilor încredere în a nu ascunde riscul cu care s-au întalnit și a cere ajutor
Bună practică 4	Părinții sunt informați și învățați cum să adopte setările de privacy sau să blocheze conturile copiilor

Monitorizare și intervenție

Standard 3.1.	Copiii sunt monitorizați în timp ce folosesc dispozitivele IT în centrul Caritas.
Criterii	
Sub-standard	● Copiii folosesc echipamentele IT din centre singuri și fără nici o formă de supraveghere.
Minim	● Atunci când utilizează tableta sau laptopul, copiii sunt supravegheați de un angajat al centrului care verifică regulat activitatea copiilor.
Bună practică 1	Angajații centrului discută în mod regulat cu copiii despre ce fac pe internet și despre experiențele lor în mediul online.
Bună practică 2	Copiii nu văd în angajatul centrului care supraveghează activitățile online o instanță de control, ci o persoană de încredere la care pot apela când este nevoie.
Bună practică 3	Există o monitorizare a timpului petrecut în mediul online și a modului de folosire a internetului (test standard) pentru depistarea cazurilor de dependență
Bună practică 4	Stabilirea unui program strict de acces la internet pe intervale de timp bine definite pentru ca monitorizarea sa fie eficientă

Standard 3.2.	Incidentele în mediul online în care sunt implicați copiii sunt documentate, discutate în echipă și informațiile relevante sunt comunicate către alte centre Caritas.
Criterii	
Sub-standard	● Incidentele de siguranță în mediul virtual sunt neglijate, rămân fără urmări și nu sunt discutate nici în echipa centrului
Minim	● Incidentele de siguranță în mediul online petrecute în centrul Caritas sunt documentate într-un registru de incidente și discutate cu echipa centrelor ● Incidentele majore care pot fi de interes și pentru alte centre Caritas sunt prezentate la întâlniri de lucru cu colegii din dieceză și din alte organizații Caritas
Bună practică 1	Există un sistem online de raportare și monitorizare a incidentelor care este folosit de toate organizațiile Caritas care au centre de zi pentru copii. Sistemul permite participanților să raporteze incidentele și să afle despre incidente și riscuri identificate în alte centre.
Bună practică 2	Incidentele petrecute în afara centrului, dar cu implicarea beneficiarilor sunt discutate și documentate în cazul în care copilul sau părinții apelează la centrul Caritas.
Bună practică 3	Incidentele petrecute în centrele Caritas sau survenite din surse externe, sunt prezentate copiilor (cu respectarea anonimatului) pentru a-i face să conștientizeze pericolele care pot exista.
Bună practică 4	Implicarea activă a copiilor cu scopul de a limita incidentele din mediul online: organizarea semestrială a unei sesiuni de joc de rol în care copiii să găsească soluții la problemele expuse.

Note de ghidare:

Formularul pentru raportarea incidentelor majore se găsește la:

https://forms.gle/VRxzuxCZvNdF2hG26

Standard 3.3.	În cazul unui incident sau abuz asupra unui copil în mediul online, echipa centrului intervine pe plan individual și în grup. Dacă este cazul, sunt implicate și autoritățile competente.
Criterii	
Sub-standard	● Centrul Caritas nu are desemnată o echipă care sa intervină în cazul unui incident și nu se implică în gestionarea incidentului.
Minim	● Incidentele de siguranță online sunt discutate și analizate de echipa centrului ● Pentru incidente grave, echipa centrului elaborează un plan de intervenție în sprijinul copilului afectat

	● Incidentele de siguranță sunt urmate de activități în grup sau individual ● Incidentele grave care intră în responsabilitatea autorităților de stat sunt raportate imediat către autoritățile competente.
Bună practică 1	În cazul în care un copil are nevoie de asistență de specialitate (de exemplu psihologică) în urma unui incident în mediul online, echipa centrului apelează la specialiști din cadrul organizației sau din alte organizații și instituții
Bună practică 2	Există la centru o listă de contacte a autorităților competente pentru abuzuri comise în mediul online
Bună practică 3	O persoană de încredere din cadrul angajaților oferă asistență tehnică pentru schimbarea parolelor, blocarea persoanelor nedorite și alte măsuri tehnice de protecție
Bună practică 4	În cazul incidentelor grave, centrul Caritas asigură acces la servicii de consiliere oferite de un specialist, de exemplu prin apelarea la un psiholog din cadrul organizației sau prin semnarea unui contract de colaborare cu un specialist extern.

Standard 4.1.	În fiecare centru Caritas în care copiii beneficiari au acces la echipamente IT și în mediul online, există un responsabil (focal point) pentru siguranța copiilor în mediul online.
Criterii	
Sub-standard	● La centru nu există o responsabilitate clar definită pentru siguranța în mediul online
Minim	● Există o persoană, numită oficial, care răspunde pentru siguranța copiilor când accesează internetul folosind infrastructură IT din cadrul centrului ● Responsabilul dispune de cunoștințele necesare în domeniul de siguranță pe internet
Bună practică 1	Responsabilul pentru siguranța online este o persoană de încredere pentru copii, la care aceștia apelează când se confruntă cu riscuri și amenințări în mediul online.
Bună practică 2	Participarea persoanei responsabile la cursuri de formare.
Bună practică 3	Responsabilul pentru siguranța online are capacitatea de a monitoriza navigarea în siguranță pe internet.
Bună practică 4	Responsabilul știe să urmeze pașii necesari pentru evitarea consecințelor nedorite.

Note de ghidare

Atribuțiile persoanei responsabilă pentru siguranța online:

- Dezvoltarea unui plan pentru siguranța pe internet
- Implementarea măsurilor tehnice de siguranță pe internet (dacă este cazul, în colaborare cu un specialist extern)
- Organizarea cursurilor despre siguranța pe internet pentru angajații, beneficiarii și părinții beneficiarilor
- Consultanță și consiliere pentru beneficiarii centrului legat de siguranța pe internet și în caz de incidente
- Monitorizarea activităților online în centru

Standard 4.2.	În fiecare centru Caritas în care copiii beneficiari au acces la echipamente IT și în mediul online, există un plan de siguranță online adaptat la situația concretă a centrului.
Criterii	
Sub-standard	● Măsurile de siguranță online nu există sau sunt luate ad-hoc și într-un mod neplanificat
Minim	● Există un plan scris pentru îmbunătățirea siguranței în mediul online în cadrul centrului ● Planul pornește de la o analiză a situației actuale ● Planul are ca bază standardele minime definite în acest document de politici
Bună practică 1	Situația centrelor în privința siguranței în mediul online este reevaluată periodic și planul este revizuit
Bună practică 2	Planul este discutat cu angajații, beneficiarii și părinții beneficiarilor
Bună practică 3	Existența unui model de plan unic pentru toate centrele și un capitol cu particularități pentru fiecare
Bună practică 4	Obligativitatea existenței planului de siguranță online ajută la atingerea standardelor minime în fiecare centru

Note de ghidare

Planul este dezvoltat de responsabilul pentru siguranța online a centrului pe baza unui template (anexă) cu participarea activă a angajaților centrului. Dacă este cazul, vor fi consultați experți din cadrul organizației (de exemplu responsabilul IT) sau experți externi.