Ministerul Educației, Culturii și Cercetării al Republicii Moldova

ORDIN

06.10.2020 nr. 1069

mun. Chișinău

Cu privire la aprobarea *Reperelor metodologice privind securitatea și siguranța online a elevilor în procesul educațional la distanță pentru instituțiile de învățământ primar, gimnazial și liceal în anul de studii 2020-2021*

În temeiul prevederilor Codului educației nr. 152/2014, art. 140, alin. (1), în vederea asigurării unui mediu sigur pentru elevi și cadre didactice în instituțiile de învățământ primar, gimnazial și liceal din Republica Moldova,

ORDON:

1. A aproba Reperele metodologice privind securitatea și siguranța online a elevilor în procesul educațional la distanță pentru instituțiile de învățământ primar, gimnazial și liceal în anul de studii 2020-2021 (Anexă).
2. Direcţia învăţământ general (dl Valentin Crudu):

- va aduce la cunoștința șefilor organelor locale de specialitate în domeniul învățământului prevederile prezentului ordin;
- va organiza, în colaborare cu CI "La Strada", formarea formatorilor cu privire la implementarea Reperelor metodologice privind securitatea și siguranța online a elevilor în procesul educațional la distanță, inclusiv online, pentru instituțiile de învățământ primar, gimnazial și liceal în anul de studii 2020-2021.

3. Organele locale de specialitate în domeniul învățământului:

- vor aduce la cunoștința directorilor instituțiilor de învățământ din subordine prevederile prezentului ordin;
- vor asigura organizarea și desfășurarea eficientă a sesiunilor de formare a cadrelor didactice din instituțiile de învățământ din subordine cu privire la implementarea Reperelor metodologice privind securitatea și siguranța online a elevilor în procesul educațional la distanță, inclusiv online, pentru instituțiile de învățământ primar, gimnazial și liceal în anul de studii 2020-2021.

4. Controlul asupra executării prezentului ordin se pune în sarcina doamnei Natalia GRÎU, Secretar de stat.

Ministru **Igor ȘAROV**

A.Prisăcaru, 022-232785

Anexă la Ordinul MECC
nr. 1069 **din** 06. 10. 2020

REPERE METODOLOGICE
privind securitatea și siguranța online a elevilor în procesul educațional la distanță pentru instituțiile de învățământ primar, gimnazial și liceal în anul de studii 2020-2021

PRELIMINARII

Siguranța online a elevilor trebuie să fie una din prioritățile personalului didactic în contextul procesului educațional la distanță. Ținând cont de particularitățile specifice ale procesului educațional în contextul crizei epidemiologice COVID-19, odată cu punerea în aplicare a oricărui model selectat la nivelul instituției de învățământ pentru organizarea procesului educațional în anul de studii 2020-2021, sarcina de a contribui la siguranța online a elevilor se va asigura prin:

- Formarea atitudinilor și deprinderilor de comportament responsabil în mediul virtual;
- Punerea la dispoziția copiilor informații, mijloace și instrumente pentru a raporta cazurile de violență online din partea semenilor și din partea adulților;
- Securizarea accesului copiilor la platformele și instrumentele web utilizate în procesul educațional la distanță.

Reperele metodologice privind siguranța online a elevilor în procesul educațional la distanță au fost elaborate în temeiul:

- Codului Educației al RM nr. 152/2014, art. 135 lit. h), k), l);
- Planul-Cadru pentru învățământul primar, gimnazial și liceal în anul de studii 2020-2021;
- Curricula la disciplinele școlare în vigoare pentru învățământul primar, gimnazial și liceal;
- Reglementărilor speciale privind organizarea anului de studii 2020-2021 în contextul epidemiologic de COVID-19, pentru instituțiile de învățământ primar, gimnazial, liceal și extrașcolar, aprobate prin ordinul MECC nr. 840 din 13.08.2020;
- Metodologia privind continuarea la distanță a procesului educațional în condiții de carantină pentru instituțiile de învățământ primar, gimnazial și liceal, aprobată prin Ordinul MECC nr. 351 din 19.03.2020;
- Standarde de dotare minimă a cabinetelor la disciplinele școlare în instituțiile de învățământ general, aprobate prin Ordinul nr. 193 din 26.02.2019.
- Instrucțiunile privind prelucrarea datelor cu caracter personal în sectorul educațional, aprobate prin Ordinul Centrului Național pentru Protecția Datelor cu Caracter Personal al RM nr. 03 din 21 ianuarie 2015.

Reperele metodologice stabilesc modul de implicare a personalului didactic și de conducere pentru a asigura securitatea și siguranța elevilor în procesul educațional la distanță, inclusiv online.

Noțiuni de bază

Siguranța online a copiilor reprezintă rezultatul unui șir de măsuri întreprinse pentru a proteja bunăstarea copilului în mediul virtual de eventuale riscuri ce îi pot afecta integritatea fizică, emoțională sau sexuală.

Violența online – utilizarea sistemelor informatice pentru a provoca, facilita sau amenința cu aplicarea violenței asupra persoanelor ce are ca rezultat sau poate provoca daune sau suferințe fizice, sexuale, psihologice sau economice și poate include exploatarea circumstanțelor, caracteristicilor sau vulnerabilității acestora[1].

Abuz online asupra copiilor – orice formă de violență fizică, emoțională sau sexuală la care sunt expuși copiii în mediul virtual sau care este facilitată de utilizarea tehnologiilor informaționale și de comunicație.

Securitatea online - rezultatul unui șir de măsuri întreprinse pentru a asigura protecția datelor, informațiilor și dispozitivelor unei persoane.

I. Formarea atitudinilor și deprinderilor de comportament responsabil în mediul virtual

1.1. La nivel instituțional, managerii educaționali din învățământul secundar general vor programa și desfășura următoarele acțiuni:

a) Vor actualiza cu includerea în Planul anual de activitate al instituției de învățământ un compartiment special cu titlul „Asigurarea protecției vieții și sănătății copiilor", în care vor fi planificate expres acțiunile menite să promoveze siguranța online a elevilor în contextul procesului educațional la distanță", reieșind din prevederile pct. 1.7 al Planului-Cadru pentru învățământul primar, gimnazial și liceal pentru anul de studii 2020-2021, aprobat prin Ordinul MECC nr. 396 din 06.04.2020.
b) Vor fi programate și desfășura următoarele activități extracurriculare:

Ziua Internațională a Siguranței pe Internet (marcată anual în a doua zi de marți din luna februarie), în cadrul căreia se vor desfășura activități de informare și sensibilizare privind riscurile online, consolidarea culturii digitale și sporirea nivelului de conștientizare privind amenințările din mediul virtual, precum și modalitățile de protecție pe Internet pentru elevi, cadre didactice și părinți.

Lunarul securității cibernetice (marcat anual în luna octombrie), în cadrul căruia se vor desfășura activități de informare despre riscurile online și modalitățile de protecție pe Internet, pentru elevi, cadre didactice și părinți.

1.2. Cadrele didactice vor forma elevilor claselor I-XII atitudini și deprinderi de comportament responsabil online în cadrul următoarelor discipline:

- *Educația tehnologică*, aria curriculară *Tehnologii*, Modulul *Educația digitală*, conform Curriculumului;
- *Dezvoltare personală*, aria curriculară *Consiliere și dezvoltare personală*, modulul *Securitatea personală*, conform Curriculumului;
- Disciplina opțională *Educația pentru Media*, Modulul *Multimedia și noile medii în viața copilului, Consumatorul avizat și noile media* și *Mediul virtual și efectele acestuia*, conform Curriculumului.

1.3. De asemenea, în contextul formării la elevi a competențelor transversale/transdisciplinare, dezvoltarea comportamentelor sigure în mediul online se va realiza și în baza principiului integrat, la toate disciplinele școlare. Cadrele didactice vor explora oportunitățile oferite de curricula la

[1] Conform definiției Comitetului Convenției privind criminalitatea informatică, Grupul de lucru privind agresiunea cibernetică și alte forme de violență online, în special împotriva femeilor și copiilor, disponibil la https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914

disciplinele *Informatică, Educația pentru Societate, Educația civică, Limba română etc.* pentru formarea la elevi a atitudinilor și deprinderilor indispensabile unui comportament responsabil în mediul virtual, utilizând seturile didactice și varietatea tehnologiilor educaționale disponibile.

1.4. Dirigintele va realiza următoarele activități:

a. În cazul în care nu predă disciplina Dezvoltare personală, realizează cel puțin o dată pe lună o activitate despre siguranța online cu elevii conform planul de activitate anual al instituției de învățământ, în acord cu particularitățile educaționale ale clasei, cu specificul vârstei și cu interesele/solicitările elevilor, în colaborare cu alte instituții și organizații.
b. La ședințele cu părinții, în funcție de specificul de vârstă al copiilor, discută despre:
   - comportamentele copiilor în mediul online în funcție de vârstă și posibilele riscuri asociate acestora;
   - importanța comunicării prietenoase a părinților cu copiii despre interese în mediul online, conținuturi publicate sau/și distribuite, prieteniile în mediul online;
   - observarea comportamentului copilului și a posibilelor semne că acesta ar putea trece printr-o situație neplăcută în mediul online/abuz în mediul online;
   - resurse și informații despre siguranța online, precum și instrumente pentru a cere consiliere și ajutor în cazul existenței unei situații sau situații suspecte de abuz a copilului în mediul online.
c. În contextul procesului educațional la distanță, monitorizează comportamentul elevilor în timpul activităților școlare și extrașcolare în mediul virtual;
d. Observă sistematic bunăstarea copilului online, evaluează, planifică și realizează intervenția primară;

1.5. În proiectarea didactică a activităților despre siguranța online, cadrele didactice vor ține cont de următoarele aspecte:

- Scopul activităților despre siguranța online este de a dezvolta abilități de gândire critică a copiilor în mediul online.
- Obiectivele educaționale vizează formarea de comportamente online centrate pe respect, responsabilitate și evaluare a posibilelor riscuri.
- Resurse educaționale trebuie să fie selectate în funcție de recomandările specialiștilor, specificul de vârstă al copiilor și grupul țintă căruia îi sunt adresate.
- Strategiile didactice trebuie să fie selectate în funcție de specificul de vârstă al elevilor, specificul și particularitățile de învățare și interese.
- Fiecare cadru didactic va selecta forme de evaluare a activităților didactice desfășurate, orientându-se spre identificarea în continuare a necesităților elevilor cu referire la achiziționarea de abilități pentru a face față diferitor situații în mediul online.

1.6. Cadrele didactice care desfășoară activități didactice la distanță, inclusiv online, prin intermediul unei sau mai multor platforme web, trebuie să întreprindă următoarele acțiuni în vederea prevenirii diferitor tipuri de riscuri online pentru bunăstarea copilului:

a. Să organizeze o dată pe lună discuții cu elevii despre siguranța lor online și să analizeze studii de caz cu referire la situații de abuz în mediul online care pot avea loc atât în activități online personale, cât și în activități legate de procesul educațional, cum ar fi:
   ✓ hărțuire online din partea semenilor cunoscuți sau alte persoane necunoscute;

- ✓ expunere la conținuturi cu caracter sexual sau/și violent din partea semenilor cunoscuți sau alte persoane necunoscute;
- ✓ șantaj și manipulare din partea persoanelor cunoscute sau necunoscute;
- ✓ impunerea copilului la diferite tipuri de acțiuni cu caracter sexual în mediul online.

La realizarea acestor activități, se va ține cont de prevederile curriculumului și pot fi utilizate și scenariile didactice elaborate de CI *La Strada* în coordonare cu MECC, disponibile pe www.siguronline.md, la rubrica Educatori/profesori, resurse didactice.

b. Să nu distribuie pe rețele sociale sau alte platforme secvențe foto sau/și video din timpul lecției în care elevii pot fi identificați, fără acordul scris al părintelui;
c. Să discute cu elevii despre necesitatea protejării datelor cu caracter personal în mediul online și a celor ce țin de activitățile didactice organizate în timpul procesului educațional la distanță, inclusiv online.

II. Punerea, la dispoziția copiilor, a informațiilor și a instrumentelor pentru a raporta cazurile de violență online din partea semenilor și din partea adulților;

3.1. Cadrele didactice vor informa elevii despre faptul că orice conținut online (mesaj, comentariu, fotografie, video etc.) care îi aparține și a fost distribuit fără acordul său, mesaje denigratoare sau jignitoare, acțiuni de intimidare, conturi false create cu datele sale personale, acțiuni de șantaj, comentarii urâte sau cu tentă sexuală poate fi înlăturat prin raportarea acestora pe platforma unde au fost publicate. Fiecare serviciu sau platformă online are anumite reguli de utilizare, termeni de utilizare și proceduri de raportare a conținutului abuziv online.

3.2 Cadrele didactice vor informa elevii despre serviciile alternative de raportare și consiliere online în situații de abuz online, cum ar fi: www.siguronline.md – serviciu de consiliere online a copiilor în situație de abuz online; telefonul copilului: 116-111, linia verde a Ministerului Educației, Culturii și Cercetării https://mecc.gov.md/ro/content/formularul-verde-siguranta-educatie-covid-19.

3.3. Elevii vor fi orientați să comunice dirigintelui despre orice caz suspect referitor la o situație personală în mediul online, precum și a colegilor săi.

3.5. În condițiile procesului educațional la distanță, dirigintele examinează toate cazurile suspecte de violență față de copil în mediul virtual și, în funcție de situația identificată, va aplica următoarele strategii de intervenție, conform scenariilor descrise mai jos:

a. Cadrul didactic observă sau este informat de către elevi despre conectarea unor persoane străine, neidentificate pe platforma web (De exemplu: O persoană necunoscută de către elev s-a conectat la activitatea didactică pe platformă; În chat-ul platformei apar comentarii de la un utilizator neidentificat; Elevul a primit un link de acces pentru activitatea didactică de la un utilizator pe care nu îl poate recunoaște; Un utilizator necunoscut solicită accesul la lecția desfășurată de către profesor pe platformă; Sarcinile didactice încărcate pe platforma web sunt șterse sau blocate; În clasa virtuală sunt identificate fișiere care nu par să aparțină elevilor etc.)

Cadrul didactic:

- va verifica sau va apela la ajutorul unui specialist din instituția de învățământ pentru a verifica dacă contul de pe care este organizată activitatea didactică pe platformă are setate toate măsurile de securitate pentru a înlătura problema;
- va apela inclusiv la ajutorul altor specialiști: psiholog școlar, administrație, polițist, servicii de consiliere și raportare a cazurilor de abuz a copilului, în cazul în care se identifică o situație neplăcută în care elevul deja a fost implicat.

b. *Cadrul didactic este martor, împreună cu întreaga clasă de elevi, la o situație de abuz a unui elev sau mai mulți elevi în timpul activității didactice pe o platformă web;*

1. Va ruga elevii, utilizând un chat comun sau direct, să se deconecteze de la lecție și să nu să se conecteze la același link.
2. Cadrul didactic poate încerca să identifice numele de utilizator al persoanei care s-a conectat și a întreprins acțiuni abuzive la adresa elevilor sau/și a cadrului didactic, poate face captură de ecran în cazul în care au fost făcute partajări de ecran cu conținuturi dăunătoare pentru elevi.
3. Urmare a incidentului, psihologul școlar va pregăti un plan de lucru cu clasa de elevi/elevul în care a avut loc situația.
4. Instituția de învățământ va colabora cu organele competente sau/și cu servicii de consiliere și raportare pentru a preveni alte posibile situații de abuz online în timpul lecțiilor la distanță, inclusiv online, sau în afara acestora.

c. *Cadrul didactic află despre un caz suspect de violență online asupra copilului care nu are legătură cu procesul educațional la distanță* [2];

Caz mai puțin grav de violență online

- Distribuirea unor fotografii redactate ale copilului, meme-uri pentru a arăta urât;
- Publicarea unor comentarii neplăcute la postările copilului pe rețele sociale din partea colegilor sau semenilor;
- Primirea unui mesaj neplăcut de la cineva etc.

Cadrul didactic va întreprinde următoarele acțiuni:

1. Va discuta cu elevul ce a trecut prin această experiență de violență;
2. Va recomanda/va ajuta copilul să raporteze comentariul, fotografia, conținutul neplăcut pe platforma web pe care a fost publicat și să blocheze utilizatorul/ utilizatorii care manifestă comportamente răutăcioase, dacă sunt persoane necunoscute;
3. *Va anunța administrația instituției de învățământ despre situație/ persoană responsabilă desemnată de instituție;*
4. Va avea discuții constructive cu alți elevi implicați în situație;
5. Va informa părinții copilului supus situației de violență despre acțiunile comise față de el, consecințele acestora, măsurile întreprinse de angajații instituției de învățământ și va încuraja părintele să nu pedepsească copilul și să nu-l blameze, dar dimpotrivă să-l ajute să depășească această situație;
6. Va observa și monitoriza, în continuare, comportamentul și starea emoțională a copilului/copiilor;
7. În cazul în care inițiatorul violenței este un copil din aceeași clasă, va discuta și cu acel elev și cu părinții acestuia, conform procedurilor aplicabile în cazurile de violență în instituția de învățământ;
8. La necesitate, va invita un psiholog în lucrul cu elevii/copiii implicați în situație.

[2] La clasificarea cazurilor de violență online s-a ținut cont de categoriile privind gravitatea situațiilor de bullying stabilite în studiul privind Bullying-ul în rândul adolescenților din Republica Moldova, realizat de Sociopolis, la cererea UNICEF Moldova, Chișinău 2019.

Caz de gravitate medie de violență online

- În internet, pe rețele de socializare au fost distribuite minciuni, bârfe, lucruri denigratoare despre copil;
- Copilul primește mesaje jignitoare de la persoane cunoscute sau necunoscute, sau conturi false;
- Publicarea fără acordul copilului a unor fotografii ce îl reprezintă în ipostaze intime (De ex. în lenjerie intimă ori în costum de baie);
- Au fost create conturi false cu datele persoanele ale copilului;

Cadrul didactic va întreprinde următoarele acțiuni:

1. Va discuta cu elevul care a trecut prin această experiență de violență;
2. Va sesiza administrația instituției de învățământ și coordonatorul acțiunilor de prevenire, identificare, raportare, referire și asistență în cazurile de violență față de copii;
3. Va recomanda copilului să raporteze conținuturile publicate sau distribuite pe platforma web;
4. Dacă situația are legătură cu un caz de bullying sau violență în instituția de învățământ, va aborda toți actorii implicați conform procedurilor aplicabile în cazurile de violență în instituția de învățământ;
5. Va informa părinții copilului supus situației de violență despre acțiunile comise față de el, consecințele acestora, măsurile întreprinse de angajații instituției de învățământ și va încuraja părintele să nu pedepsească copilul și să nu-l blameze, dar, dimpotrivă, să-l ajute să depășească această situație;
6. La necesitate, va implica un psiholog în lucrul cu elevii/copiii implicați în situație.
7. În caz de necesitate, va referi la servicii copilul și părinții acestuia.

Caz grav de violență online

- A fost amenințat pe internet, pe rețele de socializare, de către persoane pe care le cunoaște ori de către persoane necunoscute;
- În internet, pe rețele de socializare, s-au făcut glume la adresa copilului, cu tentă sexuală ori a primit unele comentarii, propuneri sau conținuturi (video sau fotografii) cu caracter sexual;
- Publicarea în mediul online a unor fotografii sau video ce reprezintă copilul în ipostaze sexuale (fără lenjerie intimă, simulând sau implicat în acțiuni cu caracter sexual etc.);
- Amenințarea sau șantajul copilului (sextortion) cu distribuirea unor informații compromițătoare despre acesta, în schimbul unor acțiuni cu caracter sexual etc.

Cadrul didactic va întreprinde următoarele acțiuni:

1. Va discuta cu elevul ce a trecut prin această experiență de violență;
2. Va anunța imediat administrația instituției și coordonatorul acțiunilor de prevenire, identificare, raportare, referire și asistență în cazurile de violență față de copii;
3. Psihologul școlar va pregăti un plan de lucru cu elevul/clasa de elevi în care a avut loc situația.
4. Va informa părinții copilului supus situației de violență despre acțiunile comise față de el, consecințele acestora, măsurile întreprinse de angajații instituției de învățământ și va

încuraja părintele să nu pedepsească copilul și să nu-l blameze, dar dimpotrivă să-l ajute să depășească această situație;

5. Va informa elevii și părinții despre posibilitățile de accesare a Serviciilor de asistență psihologică și de sănătate, de dezvoltare personală și socială etc.;
6. Instituția de învățământ va colabora cu organele competente sau/și cu servicii de consiliere și raportare pentru a preveni alte posibile situații de abuz online în timpul lecțiilor la distanță sau în afara acestora.

1.6 În condițiile procesului educațional la distanță, inclusiv online, personalul didactic va aplica aceleași principii și reguli de comunicare cu copilul victimă a unei situații de violență online ca și în cazurile violenței în instituția de învățământ.

IV. Securizarea accesului copiilor la platformele și instrumentele web utilizate în procesul educațional la distanță;

4.1. Pentru a asigura accesul securizat al copiilor la platformele și instrumentele web utilizate în procesul educațional la distanță, **conducătorul instituției** va realiza următoarele acțiuni:

- Va recomanda cadrelor didactice utilizarea unor platforme educaționale și de comunicare la distanță autorizate în scopuri educaționale;
- Va organiza instruirea cadrelor didactice privind măsurile de securitate și confidențialitate a platformelor web recomandate și utilizate în scopuri educaționale, pentru ca fiecare cadru didactic să cunoască cum să prevină situațiile în care persoane străine ar putea accesa sesiunile de discuții online, să blocheze opțiunile video, audio sau chat și să evite expunerea informațiilor personale ale sale și ale elevilor în procesul educațional la distanță;
- În cazul producerii unui incident, administrația instituției de învățământ va informa organul local de specialitate în domeniul învățământului despre acțiunile întreprinse imediat/cine a fost informat;
- Urmare a incidentului instituția de învățământ:
  - va realiza o anchetă internă;
  - va realiza discuții cu copii/părinții cu dirigintele și psihologul instituției/specialistul SAP;
  - va informa OLSDÎ despre măsurile întreprinse;
  - va asigura informarea copiilor despre asistența oferită de serviciul telefonul copilului 116111 (afișarea telefonului copilului în instituție), siguronline.md și 12plus.md;
  - va asigura întocmirea și transmiterea autorității tutelare locale a fișei de sesizare a cazului de abuz, neglijare, exploatare sau trafic al copilului și a copiei fișei coordonatorului ANET, în cazul în care fișa în termen de 24 ore nu a fost transmisă autorității tutelare locale cu mențiunea cauzei netransmiterii.

4.2. Pentru a limita vulnerabilitățile de securitate pentru activitățile online și a diminua din riscurile de siguranță și securitate pentru copii, în procesul educațional la distanță, **cadrele didactice** vor realiza următoarele acțiuni:

- Vor utiliza doar platforme educaționale și de comunicare la distanță autorizate în scopuri educaționale, bine cunoscute, descărcate de pe site-uri oficiale.
- Vor studia foarte bine aplicațiile/platformele utilizate, toate opțiunile ce le oferă acestea.
- La programarea unei sesiuni online, cadrele didactice vor seta funcțiile de securitate ale platformei utilizate: ID conferință, parolă de acces, blocare acces nedorit etc.

- Invitația de participare care conține link-ul de conectare, ID sesiune și parolă vor fi transmise doar pe un canal sigur de comunicare.
- Vor evita comunicarea cu elevii pe platforme de socializare (de ex. Facebook, instagram, odnoklassniki, etc.) și va utiliza doar grupuri special create în acest scop pe platformele utilizate în scopuri educaționale (de ex. Instrumentele Google pentru Educație din pachetul G Suite).
- Vor stabili o parolă pentru fiecare sesiune online de discuții cu elevii, pentru a preveni accesul persoanelor neautorizate.
- Vor urmări discuțiile pe chat-ul comun și în cazul unor discuții neadecvate, va interveni imediat prin oprirea/blocarea chat-ului și părăsirea platformelor. În cazul în care vor identifica o situație de hărțuire în mediul online în timpul lecției online, vor fi aplicate recomandările specificate la pct. III.
- Conectarea la sesiunea online se va realiza cu câteva minute înainte. Nu se permite conectarea elevilor înaintea cadrului didactic. Dacă aplicația permite, se va activa opțiunea Waiting Room (sală de așteptare). Această funcție permite gazdei (profesorului) să controleze când sau ce participant se alătură sesiunii. În calitate de gazdă a întâlnirii, cadrul didactic poate admite sau elimina participanți unul câte unul.
- La începerea sesiunii, cadrul didactic va verifica identitatea fiecărui participant, iar în cazul unui participant necunoscut i se va respinge participarea.
- În cazul în care în sesiune a apărut un intrus care interferează video și sonor peste conținutul lecției, se vor bloca imediat toate microfoanele și camerele video, și se va opri sesiunea. Orice astfel de incident trebuie semnalat conducerii instituției/ persoanei desemnate de conducerea instituției de învățământ.
- Ca și administrator de sesiune, cadrul didactic poate activa/ dezactiva imaginile celor conectați. Pentru un grup relativ restrâns de participanți, cum este cazul elevilor dintr-o clasă, pot fi lăsate camerele video active.
- În cazul în care este înregistrată lecția pentru a fi disponibilă online, se vor dezactiva imaginile video, se va asigura că nu sunt afișate date cu caracter personal.
- Nu se va permite înregistrarea sesiunii de către participanți. Elevilor li se comunică despre faptul că doar profesorul poate controla înregistrarea, care va fi ulterior partajată cu toți cei interesați.
- La finalizarea lecției, cadrele didactice nu vor închide sesiunea până nu se vor asigura că toți elevii participanți de la distanță se deconectează de la platforma de comunicare.
- Cadrele didactice au datoria să gestioneze cu responsabilitate listele cu numele și adresele de e-mail ale elevilor.
- Listele elevilor cu datele personale vor fi păstrate doar pe echipamente dotate cu toate elementele de siguranță.
- Nu vor fi trimise liste cu date personale ca atașamente de e-mail ne-parolate.
- Cadrele didactice vor explica elevilor că următoarele acțiuni ale unei persoane din spațiul Internet în raport cu copilul reprezintă un abuz și vor încuraja elevii să comunice cazurile respective, în care:
  - o persoană poartă discuții cu conținut sexual ori intim cu elevul, fie prin mesaje textuale, fie prin mesaje audio/video, ori prin apeluri audio/video, sau prin alte modalități;
  - o persoană solicită copilului ca acesta să-i transmită imaginile foto/video intime, indiferent dacă le primește sau nu;
  - o persoană transmite copilului imagini foto/video cu conținut sexual sau linkuri către astfel de conținut;
  - o persoană îndeamnă ori impune copilul la acțiuni cu caracter sexual sau intim, fie în mediul virtual, fie îi solicită întâlnire fizică pentru același scop;

- Cadrele didactice vor explica elevilor să nu spună persoanelor necunoscute din Internet numele său, adresa, numărul telefon, datele privind conturile sale din rețelele de socializare, sau alte date personale;
- Vor explica elevului că în caz de abuz online, acesta poate fi consultat gratuit, inclusiv în mod anonim, prin următoarele modalități:
  - Telefonul copilului: 116-111
  - Web site: https://siguronline.md, https://12plus.md/

Se recomandă cadrelor didactice să studieze ***Ghidul pentru profesioniști „Ce este exploatarea sexuală online a copiilor"***, elaborat de CI „La Strada", resursele plasate pe site-ul Ministerului Educației, Culturii și Cercetării https://mecc.gov.md/ro/content/siguranta-copiilor-internet, manualele ***Educația media*** de pe platforma https://educatia.mediacritica.md/ro/ , precum și alte resurse disponibile pe site-ul https://siguronline.md.

În cazul în care a fost identificată o persoană necunoscută / s-a produs un incident de spargere a orei, un abuz online asupra elevului, profesorul îl RAPORTEAZĂ prin următoarele modalități:

- Anunțarea incidentului administrației instituției/ persoanei responsabile desemnate de conducerea instituției de învățământ;
- Anunțarea organelor abilitate prin una din mijloacele:
  - Telefon: 116-111; (022) 577-177; 112;
  - E-mail: diii.ini@igp.gov.md
  - Web site: siguronline.md, 12plus.md, politia.md

ATENȚIE! Necomunicarea cazurilor de abuz în mediul online asupra elevilor facilitează victimizarea copiilor de către abuzator. În spatele unui copil victimă întotdeauna sunt și alți copii abuzați.

4.3. Cadrele didactice vor discuta cu elevii despre platformele web utilizate în timpul activităților la distanță, referindu-se la următoarele aspecte:

a. *Funcționalitatea acestora* (cum funcționează platforma și în ce scopuri va fi utilizată);
b. *Setările de securitate necesare și obligatorii*
   1. Elevii vor fi atenționați să nu acceseze link-uri sau documente atașate suspicioase, chiar dacă par a fi expediate de către prieteni. Ar putea conține viruși, programe spyware sau malware pe computer, care să compromită securitatea acestuia.
   2. Părinții vor fi solicitați să verifice dacă au programe anti-virus sau unele software de securitate pe internet instalate pe dispozitivele digitale utilizate de către copil în procesul educațional la distanță.
   3. Elevilor și părinților li se vor explica despre modalitățile de desfășurare a lecției la distanță și contul pe care ar trebui să i se creeze copilului, atenționându-i cu privire la datele personale pe care ar trebui să le indice pe platforma web.
c. *Modalități de conexiune la activitatea/lecția online prin platformă/platforme*

   De exemplu: Înainte de a expedia link-ul pentru lecția online, cadrele didactice se vor gândi la aspectele: Cui transmite linkul pentru conectare și cum îl transmite. Cine vede acest link pentru a evita ca acesta să ajungă la persoane străine. Cum se conectează elevul și dacă elevul transmite sau nu transmite linkul unei alte persoane, cum ar fi un coleg de clasă sau o rudă a colegului de clasă. Cui se adresează elevul în cazul în care nu se poate conecta? Cui se adresează profesorul în cazul în care are probleme de ordin tehnic?
d. *Reguli clare de utilizare a platformei în timpul activității online*

De exemplu, cine face distribuire de ecran, cine permite accesul în lecție pe platformă. De către cine și pentru ce este utilizat chat-ul platformei. Cine poate părăsi lecția și pentru care motive. Numele cu care se conectează fiecare participant). Cadrul didactic își va asuma responsabilitatea de a fi moderatorul platformei care permite sau restricționează accesul la activitate, permite distribuirea de ecran, hotărăște cine părăsește platforma în timpul lecției etc.

4.4. **Organele locale de specialitate în domeniul învățământului** vor realiza următoarele acțiuni:

- solicita informația privind incidentele similare, ce au avut lor începând cu declararea stării de urgență în legătură cu situația pandemică COVID-19.
- vor organiza/conlucra cu partenerii în vederea instruirii cadrelor didactice cu privire la
    - asigurarea mediului sigur virtual pentru copii;
    - securitatea cibernetică;
    - abordarea riscurilor nou-identificate;
    - lucrul cu copii/conlucrarea/implicarea psihologului/specialistului SAP;
    - lucrul cu părinții/reprezentanții legali;
    - prevenirea cazurilor de bulling.
- vor propune discuția periodică a subiectului violenței împotriva copilului pentru agenda Consiliului Raional/municipal pentru protecția drepturilor copilului în scopul identificării și soluționării problemelor de conlucrare intersectorială.

4.5. **Coordonatorul ANET**:

- va colecta informația despre incidentele produse în mediul online:
    - în cadrul orelor realizate în regim online;
    - în afara orelor, dar care țin de incidente conexe siguranței copilului în mediul online;
- va întocmi /transmite fișa de sesizare a cazului suspect de violență, neglijare, exploatare și trafic al copilului întocmită de instituția de învățământ autorității tutelare locale/ teritoriale pentru înregistrare și întreprindere, după caz a acțiunilor ce se impun în vederea asistenței copilului;:
- va informa MECC despre incident și acțiunile imediate întreprinse în termen de 3 zile lucrătoare.

V. Aspecte tehnice cu privire la combaterea abuzului și blocarea încercărilor de deturnare a lecțiilor online

5.1. Utilizarea în siguranță a aplicației ZOOM

Măsuri organizatorice:

- Cadrul didactic va crea/iniția lecția online (Zoom Meeting) de pe contul personal Zoom;
- Toți participanți la lecție online se vor autentifica cu Nume+Prenume real, nu vor fi acceptate „nickname-uri";
- Lecția online (Zoom Meeting) **nu** se va lăsa nesupravegheată de profesor, chiar și pe timp de pauză. La finalizarea lecției sau în pauză, profesorul va opri sesiunea (**End > End Meeting for All**), iar după revenire va reporni lecția cu reconectarea tuturor elevilor;

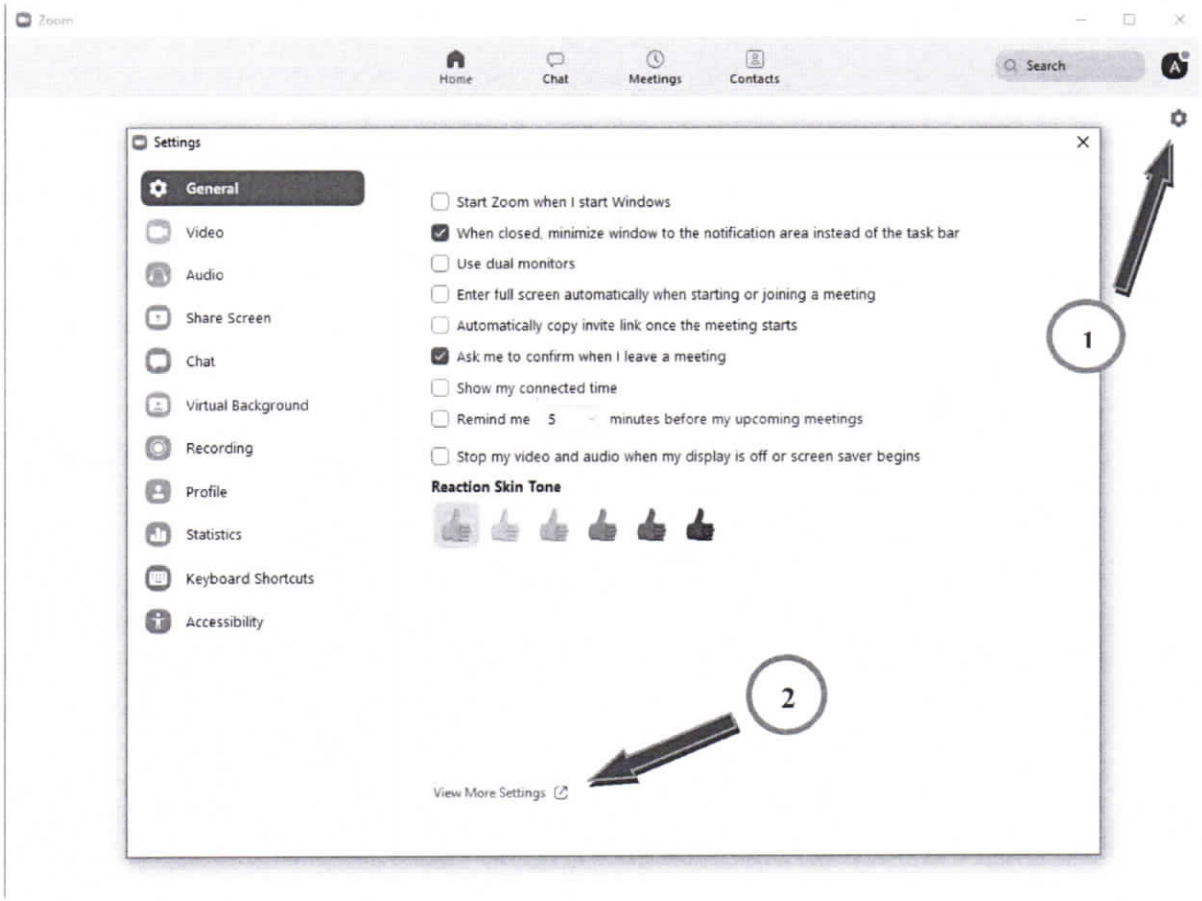
- Este interzisă distribuirea link-ului către lecția online (Zoom Meeting) persoanelor neautorizate, inclusiv celor pe care elevii îi cunosc personal.

Măsuri tehnice:

- Actualizăm aplicația – descărcăm ultima versiune.
- Evitați autentificarea prin Facebook. Problemele de securitate permit accesul la datele dumneavoastră personale.

Setări de securitate în Zoom:

Pentru a seta unele opțiuni ce ar asigura securitatea lecției online, accesați în Zoom meniul Setări (simbolul Roată dințată ⚙) > View More Settings > (se deschide profilul în browser)



În profilul din browser accesați meniul Settings > Meeting >

1) Waiting Room > (**Activare**)

***Explicație**: Când participanții se conectează la o lecție online, sunt plasați în lista de așteptare și fiecare este admis de administrator (host). Activarea listei de așteptare dezactivează automat conectarea la lecție înainte de administrator (host).*

1) Require a passcode when scheduling new meetings > (**Activare**)
   Se cere introducerea parolei pentru conectarea participanților.
2) Embed passcode in invite link for one-click join > (**Dezactivare**)
   Dezactivarea opțiunii de conectare prin accesarea link-ului fără parolă.

3) Only authenticated users can join meetings from Web client > (**Activare**)
Conectarea participanților prin Web browser este posibilă numai după autentificare în Zoom.

4) Participants video > (**Activare**)
La conectare, participantul pornește automat video și este vizibil cine se conectează.

5) Join before host > (**Dezactivare**)
Dezactivarea conectării la lecție online înainte de administrator (host).

6) Sound notification when someone joins or leaves > (**Activare**)
(Bifă) Host and co-hosts only
Administratorul primește notificare la conectarea/deconectarea unui participant.

7) Dacă nu faceți transfer de fișiere, atunci dezactivați funcția:
File transfer > (**Dezactivare**)
Nimeni nu va putea transmite fișiere în chat, inclusiv administratorul (host).

8) Dacă elevii nu fac partajarea ecranului personal, atunci lăsați funcția activată doar pentru profesor („host"):
a) Screen sharing > (**Activare**)
(Bifă) Host Only > Save
b) Disable desktop/screen share for users > (**Activare**)
Doar administratorul poate face demonstrarea ecranului.

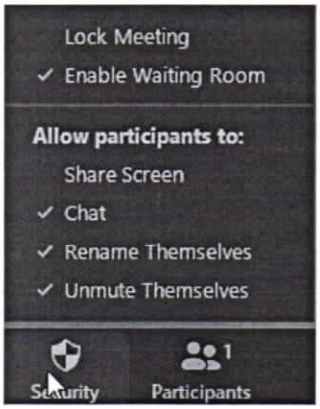
9) Remote control > (**Dezactivare**)
Dezactivarea controlului de către participanți a conținutului demonstrat de administrator.

10) Allow removed participants to rejoin > (**Dezactivare**)
Dezactivarea posibilității de reconectare pentru utilizatorii care au fost eliminați (deconectați) din lecția online de către administrator.

11) Report participants to Zoom > (**Activare**)
Administratorul poate raporta către Zoom comportamentul inadecvat al participanților. Opțiunea poate fi găsită în iconița Securitate (sub formă de scut) în timpul sesiunii Zoom (Zoom Meeting).

În profilul din browser accesați meniul Settings > Recording >

1) Automatic recording > (**Activare**)
Lecția online se înregistrează automat. Înregistrarea se va salva după finisarea sesiunii Zoom. Selectați mapa în care se va salva fișierul video.



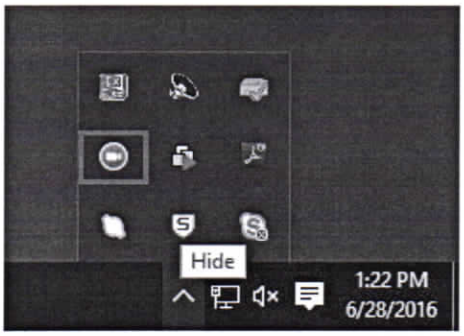
În timpul sesiunii video - în meniul „Security":

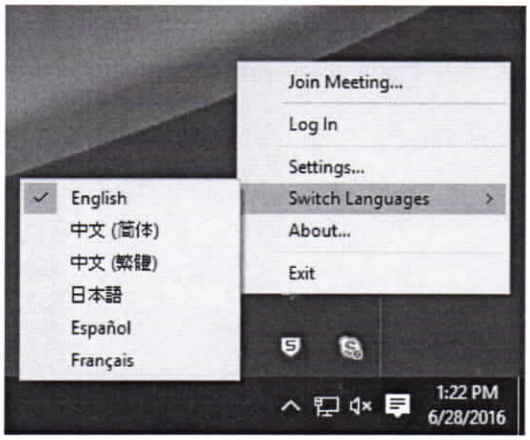
1) Verificăm să fie (**Bifă**) Enable Waiting Room
(Lista de așteptare e activată)

2) Dacă elevii nu fac prezentarea ecranului personal:
Verificăm să fie (**Debifat**) Share Screen

Selectarea limbii pentru aplicația Zoom:

1)


2)


3)


5.2. Utilizarea în siguranță a aplicației Google Meet

Controalele de securitate Google Meet sunt activate în mod prestabilit, astfel încât, în majoritatea cazurilor, utilizatorii nu vor trebui să facă nimic pentru a se asigura că sunt protejate corect.

Participanții externi nu se pot alătura sesiunilor online decât dacă fac parte din invitația din calendar sau au fost invitați de participanți. În caz contrar, trebuie să solicite aderarea la ședință, iar cererea lor trebuie acceptată de gazdă, adică de profesor.

Doar administratorul (gazda) poate dezactiva sau elimina alți participanți. Acest lucru asigură ca profesorul să nu poată fi eliminat sau dezactivat de către alți participanți.

Doar administratorul (gazda) poate aproba cererile de participare făcute de participanți externi. Aceasta înseamnă că elevii nu pot permite participanților externi să se alăture prin intermediul videoclipului și că participanții externi nu se pot alătura sesiunii.

Elevii nu se pot alătura sesiunii după ce ultimul participant a plecat. Aceasta înseamnă că dacă cadrul didactic este ultima persoană care a părăsit lecția, elevii nu se pot înscrie mai târziu fără ca profesorul să fie prezent.

Măsuri organizatorice:

- Cadrul didactic va crea/iniția lecția online (Meeting) de pe contul personal Google;
- Toți participanți la lecția online se vor autentifica prin contul personal Google care indică Nume+Prenume real, nu sunt acceptate „nickname-uri";
- La primirea solicitării din partea unui utilizator de a fi acceptat la lecție, cadrul didactic se va asigura că numele afișat este prezent în lista elevilor clasei. Imediat după acceptare, se va solicita participantului să-și afișeze fața pentru verificarea identității;
- Este interzisă distribuirea linkului lecției online (Meeting) persoanelor neautorizate, inclusiv celor pe care elevii îi cunosc personal.

⚠ Este necesar de luat în considerație că Google Meet, comparativ cu aplicația Zoom, la părăsirea lecției de către profesor (administrator), sesiunea rămâne activă și elevii ar putea rămâne nesupravegheați în sesiunea respectivă. Aceasta obligă cadrul didactic să fie ultima persoană care va părăsi lecția online.

Măsuri de securitate în Google Meet:

1) Lecția (Meeting) se organizează prin crearea unui link:

   > > Se copiază link-ul (nu se admite crearea lecției cu acces imediat prin apăsarea iconiței „+")

2) În cazul unui abuz, eliminați participantul:

Prima modalitate: Plasați cursorul mouse-ului pe fereastra participantului în Google Meet > Va apărea iconița „ ⊖ " pe care trebuie să o apăsați > În fereastra afișată, confirmați eliminarea participantului;

A doua modalitate: În lista participanților, plasați cursorul în drept cu numele participantului > Apăsați iconița „săgeată în jos" (v) > Apăsați „ ⊖ " (Eliminare)

3) În cazul în care participantul a început demonstrarea ecranului fără permisiune, opriți-o: În lista participanților, plasați cursorul în drept cu sesiunea de demonstrare a ecranului de către participant (unde este indicat numele participantului și cuvântul „demonstrare" luat în paranteze, în funcție de limba afișării) > Apăsați iconița „săgeată în jos" (v) > Apăsați „ ⊖ " (Eliminare).