GRĂDINIŢA CU PROGRAM PRELUNGIT MĂMĂRUŢA
CLUJ-NAPOCA, B-DUL 21 DECEMBRIE 1989, NR. 124,
TEL. /FAX: 0264430951
e-mail: gradinita42_cj@yahoo.com
NR. 765/ 21.09.2022

**Aprobat în ședinta C.A. din data de 14.09.2022**
**Prelucrat în ședința C.P. din data de 01.09.2022**

# POLITICA SECURITĂȚII INFORMATICE (eSafety)

Siguranța online este parte integrantă a mai multor politici ale Grădiniței cu Program Prelungit ”Mămăruța” Cluj-Napoca. Aspecte privind siguranța online se regăsesc în documente cum ar fi: *Planul de dezvoltare instituțională, Planul managerial, Planurile manageriale ale comisiilor de lucru, procedurile interne ale grădiniței, Regulamentul de ordine interioară* și *Planul de Acțiune eSafety* al grădiniței.

## 1. ARGUMENT

Politica eSafety este necesar a fi elaborată și implementată în grădiniță deoarece internetul, telefoanele, mijloacele digitale se utilizează permanent la fiecare nivel: preșcolari, profesori, personal auxiliar. Pentru a ne asigura că toți factorii implicați în educație știu să utilizeze corect și sigur oportunitățile oferite de tehnologia digitală, ei trebuie să înțeleagă și să știe să o folosească într-un mod sigur oriunde.

## 2. RESPONSABILITĂȚI

La nivelul grădiniței s-a constituit comisia pentru siguranța în mediul online și are următorii membri:

- Palfi Melania Zamfira, directorul grădiniței
- Nădejde Ramona, profesor pentru învățământul preșcolar
- Tuns Alina, consilierul de etică
- Veres Iuliana, coordonator CEAC
- Mălinaș Adriana, coordodator Structura I

Aceștia se ocupă de implementarea și monitorizarea politicii eSafety, raportând după caz directorului, cadrelor didactice și personalului didactic auxiliar și nedidactic, orice schimbare importantă în utilizarea tehnologiei, noile reglementări eSafety sau dacă este cazul discută evenimente care se petrec în grădiniță privind acest aspect, precum și organizarea evenimentelor cu ocazia **Zilei Europene a sigurantei pe internet** (februarie), precum și din cadrul **Lunii europene a securității cibernetice** (octombrie), care este o campanie anuală a Uniunii Europene menită să sensibilizeze cetăţenii şi organizaţiile cu privire la securitatea cibernetică prin furnizarea de informaţii la zi din domeniul securităţii prin intermediul educaţiei şi al schimbului de bune practici.

Siguranța în mediul online reprezintă o responsabilitate pentru orice profesor al grădiniței.

## 3. OBIECTIVE

Obiectivele privind politica eSafety a grădinței vizează următoarele aspecte:

- asigurarea relațiilor pașnice, corecte, responsabile în utilizarea noilor tehnologii în grădiniță și nu numai;
- asigurarea siguranței și securității personalului, copiilor și a părinților;
- protejarea reputației grădiniței;
- încurajarea copiilor de a utiliza tehnologia online într-un mod responsabil.

Politica eSafety este elaborată în acord cu legislaţia naţională şi internaţională, cu politicile grădiniței și are în vedere respectarea drepturilor copilului, precum şi combaterea comportamentelor antisociale şi bullying-ul. Ea a fost realizată prin implicarea şi consultarea tuturor – părinţi, personalul grădiniței, reprezentanţi ai comunităţii locale.

## 4. UTILIZAREA TELEFOANELOR MOBILE ÎN GRĂDINIȚĂ

A devenit din ce în ce mai dificil de pus în aplicare o interdicție absolută cu privire la utilizarea telefoanelor mobile, pe de-o parte deoarece acestea au devenit indispensabile în viața tinerilor, dar şi pentru că mulți părinți insistă să poată intra în orice moment în legătură cu copiii lor. Deși prezența telefoanelor mobile poate fi deranjantă și poate conduce la comportamente deranjante precum copierea şi bullying-ul, ele pot, de asemenea, să ofere oportunități fără precedent atunci când sunt utilizate în mod proactiv şi creativ în sala de clasă, atâta timp cât există o politică strictă privind deținerea și utilizarea acestora. (ROFUIP, art. 197, 2)

La Grădinița cu Program Prelungit ”Mămăruța” Cluj-Napoca există o serie de reguli pentru utilizarea telefoanelor de către personal în cadrul grădiniței precum:

- Personalul poate utiliza telefonul mobil în interes personal, în timpul orelor de activitate doar în cazuri de extremă urgență
- Accesarea rețelor de socializare sau a altor site-uri este permisă doar în cazul în care această acțiune este relevantă pentru procesul instructiv-educativ.
- Nerespectarea acestor reguli poate conduce la sancțiuni în conformitate cu *Regulamentul de ordine interioară al grădiniței*, *Statutul elevului*, *Regulamentul cadru de organizare şi funcţionare a unităţilor din învăţământul preuniversitar*.

## 5. UTILIZAREA DISPOZITIVELOR DETAȘABILE

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

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

ale altor membri al personalului pe dispozitive detaşabile cu excepția cazului în care acest lucru este necesar în vederea executării sarcinilor ce le revin, deoarece există întotdeauna riscul ca aceste dispozitive cu informații personale pe ele să fie furate sau pierdute. Este instituită o procedură oficială de gestionare a incidentelor în cazul unor infecții malware prin utilizarea unui dispozitiv mobil sau în cazul pierderii unui dispozitiv. Aceasta din urmă este deosebit de importantă dacă dispozitivul conține informații sensibile despre preșcolari sau personal.

**6. FORMAREA – INFORMAREA PROFESORILOR PRIVIND POLITICA eSAFETY**

Pentru a fi în concordanță cu politica eSafety a grădiniței, personalul unității este informat de către coordonatorii comisiei eSafety cu privire la noile reglementări care apar în fiecare an, această informare fiind punct obligatoriu în prima ședință de Consiliu Profesoral și la nevoie se fac informări și completări dacă este cazul. Informarea cadrelor cuprinde:

- Informarea privind utilizarea imaginii copilului, a postării imaginii copiilor pe site-urile de socializare (cadru legal) și reamintirea semnării declarației de către orice părinte;
- Informare privind protecția datelor sensibile ale grădiniței și a celor personale prin crearea/reînnoirea parolelor;
- Informare privind utilizarea dispozitivelor detașabile și obligativitatea scanării fiecărui dispozitiv înaintea folosirii lui;
- Informare privind utilizarea telefoanelor ținând cont de reglementările în vigoare din ROFUIP și ROI din anul în curs;
- Informare privind procedurile de gestionare a incidentelor în cazul infectării malware dacă este cazul pentru calculatoarele grădiniței;
- Utilizarea calculatoarelor din clase doar în scopuri educative;
- Recomandări privind găsirea de resurse pe site-urile oficiale www.sigur.info și desfășurarea de activități anuale cu copii.

De asemenea, cadrele didactice sunt invitate să participe la evenimentele organizate în cadrul Lunii europene a securității cibernetice și cu ocazia Zilei Siguranței pe Internet.

**7. PROTEJAREA DATELOR SENSIBILE ÎN GRĂDINIȚĂ**

Datele sensibile din cadrul unei unităţi de învăţământ includ detaliile confidenţiale ale preşcolarilor, părinţilor şi membrilor personalului, informaţii de sănătate şi psihologice ale copiilor, salariile profesorilor şi CV-urile acestora, precum şi date privind administrarea grădiniței. Aceste informaţii pot fi stocate pe computerele locale, pe dispozitive mobile, pe servere localizate pe teritoriul grădiniței sau în alte locaţii sau pe documente printate pe o imprimantă confidenţială sau comună. Protecţia insuficientă sau dezvăluirea improprie a acestor date poate rezulta într-o încălcare a confidenţialităţii sau a legilor de protecţie a datelor.

**<u>În consecință se impun următoarele acțiuni:</u>**

- În grădiniță se actualizează sistemele de protecție antivirus pentru a evita să deveniţi o țintă a hackerilor.
- Nu se vor lăsa documente ce conţin date sensibile pe imprimanta publică sau salvate pe calculator! *Distrugeţi/ștergeți astfel de documente înainte să le puneţi în coşul de gunoi (Recycle Bin).*
- Colectaţi date sensibile doar dacă este necesar. Ingineria socială se referă la comunicări (prin intermediul site-urilor sau emailurilor) care păcălesc utilizatorul să viziteze un site web sau să execute click pe o legătură pentru a deschide un ataşament care oferă acces la informaţii confidenţiale.

**8. PROTECȚIA DISPOZITIVELOR ÎMPOTRIVA PROGRAMELOR MALWARE**

*Malware* înseamnă software dăunător care a fost proiectat cu scopul accesării unei rețele sau unui sistem de computere fără consimțământul proprietarului şi poate include viruși, viermi informatici și spyware. Odată instalat, malware-ul cauzează de obicei rezultate nedorite, care pot varia de la a fi pur și simplu intruziv sau enervant până la a compromite informații cu caracter personal în

sistem sau până la a fi pur și simplu distructiv. Malware-ul ajunge de obicei în sistemul IT al unei școli prin intermediul spam-ului, descărcării de fișiere contaminate sau prin intermediul dispozitivelor mobile infectate (USB, hard disk extern, telefon mobil, etc.).

**AȘADAR**

- În grădiniță pe fiecare calculator este instalat firewall-ul și sisteme de protecție anti-virus și se actualizează pentru a evita breșele de securitate.
- Se blochează site-urile nedorite și ferestrele de tip pop-up prin personalizarea setărilor de securitate ale browser-ului web utilizat pe computerele grădiniței prin aceasta urmărindu-se protecția lor.
- Se creează un protocol care să fie aplicat cu rigurozitate cu privire la utilizarea Internetului și verificarea mail-urilor personale pe computerele grădiniței.
- Nu se accesează din mail-uri adrese dubioase/reclame/pop-up orice care nu au legătură cu activitatea școlară.
- Se desemnează o persoană de contact instruită care să se ocupe de toate problemele legate de malware și se instituie o procedură oficială de gestionare a incidentelor informatice.

## 9. POLITICA DE UTILIZARE ACCEPTABILĂ

Reprezintă o bună practică ca şcoala să aibă o *Politică de Utilizare Acceptabilă (PU*A), adică un document clar şi concis care să ofere îndrumare unor categorii de utilizatori cu privire la felul în care ar trebui utilizate Internetul şi tehnologiile mobile. Politicile de Utilizare Acceptabilă s-au dezvoltat în timp şi este evident că copii şi personalul din şcoli au posibilitatea să acceseze Internetul în multe moduri, nu numai prin intermediul reţelei grădiniței. Având în vedere acest fapt, este important ca o Politică de Utilizare Acceptabilă să fie centrată mai mult pe comportament decât pe tehnologie. Acest lucru înseamnă că politica va avea o viaţă mai lungă şi va fi mai uşor de înţeles de către toţi cei interesaţi.

## 10. PAROLE SIGURE

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

Se amintește personalului cele 4 reguli de aur ale unui parole sigure:

- să conţină între 10 și 14 caractere;
- folosirea unuu amestec de numere, simboluri, litere mari şi litere mici și semne de punctuație;
- folosirea unui acronim pentru o frază;
- să nu se utilizeze informații personale de identificare în parolă. (Acestea includ nume, zile de naștere, animale de companie, adrese de străzi, şcoli, numere de telefon, numerele de înmatriculare etc. Acestea vor fi primele presupuneri pentru oricine încearcă să obțină acces la contul dvs.); dacă utilizatorii simt totuşi nevoie să scrie parola, aceasta nu trebuie să fie ţinută în apropierea dispozitivului la care oferă acces.

## 11. POLITICA GRĂDINIȚEI

Politicile de eSafety ale grădiniței s-au dezvoltat rapid, deoarece părțile interesate pot accesa în prezent Internetul într-o multitudine de moduri în incinta grădiniței. Suntem conștienți că avem în fața noastră generația copiilor digitali care au o afinitate aparte pentru tehnologiile digitale care fac parte din viața noastră de zi cu zi. Pentru a ne asigura că oportunitățile disponibile prin intermediul tehnologiilor digitale sunt valorificate cum se cuvine de către copiii, chiar dacă vârsta lor este relativ mică, aceştia trebuie să le cunoască și să înțeleagă cum să le folosească, acum mai mult ca niciodată.

## 12. REALIZAREA ȘI PUBLICAREA DE FOTOGRAFII ȘI CLIPURI VIDEO ÎN CADRUL GRĂDINIȚEI

Participarea preșcolarilor la anumite activități și evenimente reprezintă momente de neuitat și motive de mândrie pentru părinți – sunt momente pe care mulți vor dori să le fotografieze sau să le filmeze. Având în vedere accesul rapid de la un ecran de telefon mobil, la un site de socializare, există anumite reguli pe care conducerea şi personalul grădiniței ar trebui să le ia în considerare și să le comunice părinților.

**DREPT URMARE,** conducerea, cadrele didactice și personalul grădiniței trebuie:

- Să știe că grădinița are o politică clară referitoare la imagine şi fotografie indiferent dacă aceasta este sau nu o obligație legală în țară.
- Se comunică comunităţii şcolare această politică alături de îndrumări practice clare și exemple ușor de înțeles.
- Să se asigure că toţi membri comunităţii şcolare înțeleg implicațiile partajării fotografiilor și conținutului video pe site-urile de socializare – a nu se posta NICIODATĂ numele complet, vârsta sau orice alt detaliu personal alături de fotografia unui copil pe site.
- Să se asigure că toți părinții/tutorii legali și/sau copii (în funcție de vârstă și cerințe naționale) au bifat permisiunea de fotografiere/video ÎNAINTE de orice filmare sau fotografiere a elevilor, prevăzută în Contractul educațional care se semnează la intrarea în grădiniță:

PERMISIUNEA DE A FOLOSI IMAGINI DIN ACTIVITATEA COPILULUI

Acord permisiunea de a utiliza exclusiv în scop de marketing sau de formare profesională, imagini foto sau înregistrări video obţinute în timpul programului de activitate al grădiniţei .

## 13. PREZENȚA GRĂDINIȚEI PE REȚELELE DE SOCIALIZARE

Folosirea reţelelor de socializare de către şcoli este un subiect controversat, putând fi aduce argumente pentru şi împotrivă, de la riscul cyberbullying-ului şi prieteniile online dintre părinții copiilor şi educatoare până la promovarea activă pe care o poate aduce Facebook-ul sau Twitter-ul. De la dezvoltarea profesională până la descoperirea de exemple din viaţa reală la orele de limbi străine, socializarea media în unitățile de învățământ poate reprezenta o resursă valoroasă. Cel mai important lucru care trebuie avut în vedere în legătură cu utilizarea reţelelor de socializare în şcoli este chestiunea drepturilor şi responsabilităţilor online. Pe lângă rolul de instrument promoţional pentru grădinițe, profesorii din toată lumea au enumerat mai jos beneficiile utilizării reţelelor sociale în şcoli:

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

## 14. INTEGRAREA eSAFETY ÎN CURRICULUM

În ultimii ani TIC și mediul digital oferă preșcolarilor un potențial enorm de a explora, de a se conecta și de a crea, copii au nevoie de îndrumări suplimentare cu privire la comportamentul sigur și responsabil în mediul online. În special, ei trebuie să învețe strategii eficiente de găsire a unui

echilibru între oportunități și riscuri, de gestionare a informațiilor online și a securităţii acestora, de protejare a intimităţii lor și respectare a celuilalt, de gestionare a cazurilor de cyberbullying, de a distinge între contacte şi conţinut nepotrivit și pozitiv, ș.a.m.d.

Grădinița cu Program Prelungit ”Mămăruța” are în derulare multiple proiecte (locale, naționale, și internaționale), așa că fiecare cadru didactic indiferent de vârsta copiilor, de disciplina predată integrează eSafety în curriculum, fiind cea mai potrivită abordare pentru însușirea corectă a utilizării în siguranță.

**ÎN CONSECINȚĂ**

- Grădinița se asigură că eSafety se predă ca parte a programei (indiferent dacă aceasta constituie sau nu o obligație legală în România).
- În grădiniță se urmărește o abordare trans-curriculară mai cuprinzătoare, menită a explora numeroasele legături dintre eSafety și toate tipurile de conținut educaţional.
- Deoarece eSafety reprezintă o responsabilitate trans-curriculară, toate cadrele didactice din grădiniță beneficiază de formare periodică pe teme cum ar fi: confidenţialitatea și securitatea, amprenta digitală și reputația, cyberbullying-ul, alfabetizarea informațională etc.
- În predarea acestora și altor aspecte referitoare la eSafety trebuie pornit de la ceea ce copii știu deja și de la felul în care experimentează ei mediul online.

## 15. INFORMAȚII PENTRU PĂRINȚI

Părinții joacă un rol vital în siguranța online a copiilor. Desigur, grădinița este în măsură să adopte multe măsuri – poate filtra, monitoriza și educa, dar trebuie să recunoaștem că mulți copiii au acasă sau prin intermediul unui dispozitiv mobil un nivel foarte diferit de acces la Internet decât la grădiniță. Mulţi părinţi sunt destul de eficienţi în îngrijirea și îndrumarea copiilor cu privire la problemele offline, dar sunt reticenţi în încercarea de a le oferi sprijin similar în ceea ce privește aspectele digitale ale vieții lor. Parţial acest lucru poate fi un rezultat al faptului că mulți părinți spun despre copiii lor că “se pricep mai bine la tehnologie” decât ei.

- Grădinița cu Program Prelungit ”Mămăruța” oferă sprijin, îndrumare și consiliere pentru părinți. Acest lucru poate lua diverse forme: o discuţie specifică pe această temă, pliante despre diferite probleme, legături (link-uri) pe site-ul grădiniței sau articole în revista grădiniței ”Aventurile Mămăruței”, informări în ședințe cu părinții.
- Este important să recunoaștem că de multe ori părinții care participă la o activitate sau eveniment eSafety sunt tocmai părinții care probabil nu au nevoie să participe. Părinții interesaţi de ceea ce fac copiii lor online vor fi dornici să comunice pe aceste teme, vor fi, de asemenea, mult mai conștienți cu privire la problemele actuale ale siguranței pe internet.
- Unitățile de învățământ raportează că implicarea părinţilor în problemele eSafety poate fi o provocare și că aceştia sunt de multe ori reticenţi în a veni la grădiniță pentru astfel de evenimente. În acest caz se recomandă implicarea copiilor în livrarea acestor mesaje, deoarece părinții sunt mai înclinaţi să vină la un eveniment în care copilul lor participă direct, de exemplu, prin susţinerea unei prezentări. O altă strategie este livrarea mesajelor eSafety în timp ce părinții sunt deja în grădiniță cu alte scopuri, sedințe cu părinții, lectorate pe grădiniță, distribuire de fluturaşi, flyere despre diferite aspecte ale siguranţei în mediul on-line, promovarea de link-uri pe pagina de facebook a grădiniței, pe site-ul grădiniței, articole în revista grădiniței.

## 16.UTILIZAREA TEHNOLOGIEI ONLINE DE CĂTRE ELEVI ÎN AFARA GRĂDINIȚEI

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

**Modalități:**

- Includerea unei declarație în Politica grădiniței și în Politica de Utilizare Acceptabilă cu privire la modul în care vor fi gestionate problemele online care au loc în afara grădiniței.
- Oferirea de Informaţii părinților și copii cu privire la angajamentul grădiniței de a se ocupa de aceste tipuri de probleme.
- Organizarea în cadrul grădiniței a unor activități de creştere a gradului de conştientizare pentru a informa copii de posibilele consecințe ale problemelor online, cum ar fi bullying-ul și încălcarea confidenţialităţii.
- Desemnarea unui profesor pe care copii îl pot consulta atunci când se confruntă cu probleme online, indiferent dacă acestea au loc la grădiniță sau în afara grădiniței. Această persoană trebuiesă fie în măsură să ofere sfaturi tehnice de bază (de exemplu, cum pot să-mi protejeze contul de Facebook), precum și consiliere psihologică (de exemplu, în cazul unui incident de cyberbullying).
- La nevoie, grădiniță trebuie să contacteze părinții tuturor elevilor implicați într-o problemă și dacă este cazul să apeleze la ajutor profesionist extern.
- Urmărirea numărului și natura rapoartelor și identificarea eventualelor nevoi specifice din grădiniță.

## 18. GESTIONAREA INCIDENTELOR

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

**ÎN ACEST SENS**

- Este important să se revizuiască incidentele la şedinţele periodice cu personalul. (imediat după incident ar putea exista o rezistenţă firească la revizuirea incidentului din partea membrilor personalului implicat. Este preferabil a se lăsaun timp de reflexie, astfel încât toată lumea să privească incidentele cu detaşare.)
- Este necesară discutarea întrebărilor din lista de control eSafety atunci când se revizuiește un incident. (Incidentul trebuie raportat prin intermediul handling report.)
- Raportarea incidentelor prin intermediul unui şablon furnizat pe site va conta în acordarea punctelor de acreditare, va rămâne anonimă și va constitui o sursă de învățăre unii de la alții.)

## 19. CYBERBULLYING

*Cyberbullying* – denumit uneori şi bullying online – este o problemă foarte complexă. Poate fi definit ca utilizarea tehnologiei și în special a telefoanelor mobile și Internetului, pentru a răni în mod deliberat, supăra, hărțui sau a jena o persoană. Acesta poate fi prelungire a intimidării faţă-în-faţă, tehnologia oferind agresorului o altă metodă de hărţuire a victimei, cu sau fără niciun motiv. Poate avea loc prin intermediul oricărei forme de media, de la mesaje şi imagini ofensatoare trimise de pe telefoane mobile, la postări neplăcute pe bloguri și pe rețelele de socializare sau e-mailuri și mesagerie instantanee, până la site-uri dăunătoare create numai cu scopul de a intimida o persoană sau abuz virtual în timpul unui joc multiplayer online. Cyberbullying-ul diferă de alte forme de bullying: poate invada casa şi spaţiul personal al victimei, publicul este potenţial mai numeros, mesajele sau imaginile supărătoare pot fi propagate rapid și există dificultăți în controlarea și/sau eliminarea mesajelor transmise electronic.

De asemenea, deoarece nu presupune interacţiune faţă-în-faţă, cyberbullyingului i se atribuie de obicei un caracter anonim. Acest lucru îi poate determina pe oameni să se implice în activități în care nici n-ar visa să se implice în lumea reală, fie ca autor sau ca un spectator.

**PENTRU EVITAREA ACESTOR SITUAȚII**

- Se adoptă o abordare anti-bullying la nivelul întregii grădinițe.

- Se comunică în mod clar strategia pentru toți membrii comunității școlare – copii, cadre didactice, personal didactic auxiliar, nedidactic și părinți. Toată lumea trebuie să fie conștientă de traseele de raportare și de consecințele pentru cei implicați în astfel de comportamente.
- Se revizuiește periodic strategia adoptată, se evaluează succesul acesteia și se adaptează dacă este necesar.
- Se organizează sau se încurajează participarea la formări pentru profesori.
- Se integrează în programă conştientizarea cu privire la (cyber) bullying pentru toate categoriile de vârstă.
- Se organizează sesiuni de informare pentru părinți. (Aceştia ar putea să nu fie conştienţi de noile instrumente tehnologice și de modul în care copiii lor le folosesc.)

DIRECTOR,
Prof. Palfi Melania Zamfira