

Centrul Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova Notificat Data _____	Instituția Publică Liceul Teoretic „Olimp” mun. Chișinău Aprobat Cons. de administrație nr.7 din 05.06.2020 Director _____ Vasic Elvira
--	--

POLITICA

**DE SECURITATE PRIVIND PROTECȚIA ȘI PRELUCRAREA DATELOR CU
CARACTER PERSONAL ÎN SISTEMELE DE EVIDENȚĂ**

INSTITUȚIA PUBLICĂ LICEUL TEORETIC „OLIMP”

mun. Chișinău

Cuprins

I.	PREAMBUL.....	p.2
II.	INTRODUCERE.....	p.2
III.	NOȚIUNI GENERALE.....	p.3
IV.	OBIECTIVELE POLITICII DE SECURITATE.....	p.5
V.	RESPONSABILITATEA RESPECTĂRII POLITICII DE SECURITATE.....	p.6
VI.	MĂSURILE DE PROTECȚIA DATELOR CU CARACTER PERSONAL.....	p.6
VII.	DEZVĂLUIREA DATELOR CU CARACTER PERSONAL	p.7
VIII.	DREPTURILE SUBIECȚIILOR LA DATE CU CARACTER PERSONAL.....	p.9
IX.	STOCAREA, PĂSTRAREA ȘI DISTRUGEREA DATELOR CU CARACTER PERSONAL.....	p.9
X.	AUDITUL SISTEMELOR INFORMAȚIONALE GESTIONATE...p.10	
XI.	GESTIONAREA INCIDENTELOR DE SECURITATE.....	p.11
XII.	MARCAREA DOCUMENTELOR	p.11
XIII.	RESPONSABILITATEA LEGALĂ PENTRU ASIGURAREA DATELOR CU ACARACTER PERSONAL	p.11
XIV.	DISPOZIȚII FINALE.....	p.11

I. PREAMBUL

La prelucrarea datelor cu caracter personal în cadrul entităţii sunt aplicate principiile prevăzute de actele **internaţionale**:

- Declaraţia universală a drepturilor omului;
- Convenţia cu privire la drepturile copilului;
- Convenţia pentru apărarea drepturilor omului şi a libertăţilor;
- Convenţia pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal;
- Directiva 95/46/CE a Parlamentului European şi a Consiliului privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date;

a celor **naţionale**:

- Constituţia Republicii Moldova;
- Codul Educaţiei;
- Legea privind protecţia datelor cu caracter personal nr.133, din 08.07.2011;
- Legea privind accesul la informaţie;
- Metodologia de aplicare a Procedurii de organizare instituţională şi de intervenţie a lucrătorilor instituţiilor de învăţământ preuniversitar în cazurile de abuz; neglijare, exploatare, trafic al copilului (ME nr.858 din 23.08.2013);
- Strategia pentru protecţia copilului pe anii 2014-2020 (HG nr. 434 din 10.06.2014);
- Regulamentul privind sistemul de cartografiere a şcolilor primare, gimnaziale şi liceelor, Hotărârea Guvernului nr.899 din 27.10.2014;
- Cerinţele faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr. 1123 din 14 decembrie 2010,
- Regulamentului Registrului de evidenţă al operatorilor de date cu caracter personal, aprobat prin Hotărârea Guvernului nr. 296 din 15 mai 2012 şi alte acte legislative/normative de profil.

şi a celor **la nivel de instituţie**:

- Statutul instituţiei;
- Regulamentul intern al instituţiei;
- Politica de protecţie a copilului (CA nr.2 din 07.10.2019)

XV. INTRODUCERE

Instituţa Publică Liceul Teoretic „Olimp” (în continuare – IPLT „Olimp”) are sediul înregistrat pe strada Petru Zadnipru 7/1, mun. Chişinău, Republica Moldova.

Politica este aprobată de către consiliul de administraţie a liceului, care acţionează în baza legislaţiei: Constituţia Republicii Moldova, Codul Educaţiei, Statutul IPLT „Olimp”

și alte acte normative, care nu contravin legislației în vigoare.

Prezenta Politică este aprobată, inclusiv, în vederea conformării IPLT „Olimp” cu prevederile Hotărârii Guvernului Republicii Moldova nr.1123 din data de 14 decembrie 2010 "Privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal" și Legii Republicii Moldova nr.133 din 08.07.2011 "Privind protecția datelor cu caracter personal".

III.NOȚIUNI GENERALE

În prezenta Politică de Securitate, sunt definite/utilizate următoarele noțiuni:

date cu caracter personal - orice informație referitoare la o persoană fizică identificată sau identificabilă (subiect al datelor cu caracter personal). Persoana identificabilă este persoana care poate fi identificată, direct sau indirect, prin referire la un număr de identificare sau la unul ori mai multe elemente specifice identității sale fizice, fiziologice, psihice, economice, culturale sau sociale;

categorii speciale de date cu caracter personal - datele care dezvăluie originea rasială sau etnică a persoanei, convingerile ei politice, religioase sau filozofice, apartenența socială, datele privind starea de sănătate sau viața sexuală, precum și cele referitoare la condamnările penale, măsurile procesuale de constrângere sau sancțiunile contravenționale;

prelucrarea datelor cu caracter personal - orice operațiune sau serie de operațiuni care se efectuează asupra datelor cu caracter personal prin mijloace automatizate sau neautomatizate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, păstrarea, restabilirea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ștergerea sau distrugerea;

operator (responsabil) - persoana fizică sau persoana juridică de drept public sau de drept privat, inclusiv autoritatea publică, orice altă instituție ori organizație care, în mod individual sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal prevăzute în mod expres de legislația în vigoare;

persoană împuternicită de către operator - persoana fizică sau persoana juridică de drept public ori de drept privat, inclusiv autoritatea publică și subdiviziunile ei teritoriale, care prelucrează date cu caracter personal în numele și pe seama operatorului, pe baza instrucțiunilor primite de la operator;

CCTV (closed circuit television) – sistem de supraveghere video/camere de supraveghere video de circuit închis care captează imagini video pe o arie de interes, iar imaginile pot fi vizionate în timp real pe un monitor/televizor. De asemenea, aceste imagini pot să fie înregistrare pentru o vizionare ulterioară;

destinatar – orice persoană fizică sau persoană juridică de drept public ori de drept privat, inclusiv autoritatea publică și subdiviziunile ei teritoriale, căreia îi sunt dezvăluite date cu caracter personal, indiferent dacă este sau nu terț;

sistem de evidență a datelor cu caracter personal - orice serie structurată de date cu caracter personal accesibile conform unor criterii specifice, fie că este centralizată,

descentralizată ori repartizată după criterii funcționale sau geografice. În calitate de sistem de evidență a datelor cu caracter personal se constituie inclusiv dar nu se limitează la bazele de date, sisteme informaționale și informatice în care sunt stocate și prelucrate automatizat sau manual date cu caracter personal;

depersonalizarea datelor - modificarea datelor cu caracter personal astfel încât detaliile privind circumstanțele personale sau materiale să nu mai permită atribuirea acestora unei persoane fizice identificate sau identificabile ori să permită atribuirea doar în condițiile unei investigații care necesită cheltuieli disproporționate de timp, mijloace și forță de muncă;

autentificare - verificarea identicatorului atribuit subiectului de acces, confirmarea autenticității;

control de securitate - acțiuni întreprinse de către IPLT „Olimp” în vederea asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaționale și/sau registrelor ținute;

fișiere temporare - ansamblu de date sau informații pe suport digital creat pentru o perioadă de timp limitat până la inițierea îndeplinirii sarcinilor pentru care au fost desemnate;

identificare - atribuirea unui identicator subiecților și obiectelor de acces și/sau compararea identicatorului prezentat cu lista identificatoarelor atribuite;

integritate - certitudinea, necontradictorialitatea și actualitatea informației care conține date cu caracter personal, protecția ei de distrugere și modificare neautorizată;

mijloace de protecție criptografică a informației care conține date cu caracter personal - mijloace tehnice, de program și tehnico-aplicative, sisteme și complexe de sisteme ce realizează algoritmi de conversie criptografică a informației care conține date cu caracter personal, destinate să asigure integritatea și confidențialitatea informației în procesul de prelucrare, depozitare și transmitere a acestora prin canalele de comunicații;

nivel de protecție - nivel de securitate proporțional riscului pe care îl comportă prelucrarea față de datele cu caracter personal respective, precum și față de drepturile și libertățile persoanelor, elaborat și actualizat corespunzător nivelului dezvoltării tehnologice și costurilor implementării acestor măsuri;

politica de securitate a datelor cu caracter personal - document, elaborat de către operatorul de date IPLT „Olimp”, care oferă o descriere precisă a măsurilor de securitate și trăsăturilor de protecție selectate pentru securitatea datelor, ținându-se cont de potențialele pericole pentru datele cu caracter personal prelucrate și riscurile reale la care sînt expuse acestea;

perimetru de securitate - zona care reprezintă în sine o barieră de trecere asigurată cu mijloace de control fizic și/sau tehnic al accesului;

persoana responsabilă de politica de securitate a datelor cu caracter personal - persoana responsabilă de funcționarea corespunzătoare a sistemului complex de protecție a informației care conține date cu caracter personal, precum și de elaborarea, implementarea și monitorizarea respectării prevederilor politicii de securitate a deținătorului de date cu caracter personal;

protecția informației contra acțiunilor neintenționate - ansamblu de măsuri orientate spre prevenirea acțiunilor neintenționate, provocate de erorile utilizatorului, defectele mijloacelor tehnico-aplicative, fenomenele naturii sau alte cauze ce nu au ca scop direct modificarea informației, dar care conduc la distorsiunea, distrugerea, copierea, blocarea accesului la informație, precum și la pierderea, distrugerea acesteia sau la defectarea suportului material al informației care conține date cu caracter personal;

purtător de date cu caracter personal - suport magnetic, optic, laser, de hârtie sau alt suport al informației, pe care se creează, se fixează, se transmite, se recepționează, se păstrează sau, în alt mod, se utilizează documentul și care permite reproducerea acestuia;

restaurarea datelor - procedurile cu privire la reconstituirea/prestabilirea datelor cu caracter personal în starea în care se aflau pînă la momentul pierderii sau distrugerii acestora;

tehnologie informațională - totalitatea metodelor, procedeele și mijloacelor de prelucrare și transmitere a informației care conține date cu caracter personal și regulile de aplicare a acesteia;

utilizator - persoana care acționează sub autoritatea deținătorului de date cu caracter personal, cu drept recunoscut de acces la sistemele informaționale de date cu caracter personal;

sesiune de lucru — perioada care durează din momentul pornirii calculatorului și aplicației de utilizare a resursei informaționale sau din momentul pornirii resursei informaționale și pînă la momentul opririi acestora;

sistem informațional de date cu caracter personal - totalitatea resurselor și tehnologiilor informaționale interdependente, de metode și de personal, destinată păstrării, prelucrării și furnizării de informație care conține date cu caracter personal;

stocare - păstrarea pe orice fel de suport a datelor cu caracter personal;

consimțământul subiectului datelor cu caracter personal - orice manifestare de voință liberă, expresă și necondiționată, în formă scrisă sau electronică, conform cerințelor documentului electronic, prin care subiectul datelor cu caracter personal acceptă să fie prelucrate datele care îl privesc.

IV.OBIECTIVELE POLITICII DE SECURITATE

Obiectivele principale ale Politicii sunt disponibilitatea, integritatea și confidențialitatea tuturor informațiilor, inclusiv datelor cu caracter personal prelucrate de IPLT „Olimp”, atât în cadrul procesului instructiv-educativ, cât și sistemelor și proceselor de tehnologie informațională la nivel de Minister (SIME, SIPAS, SPAD etc). Securitatea reprezintă o componentă esențială a derulării optime a proceselor bazate pe protecția datelor cu caracter personal în cadrul IPLT „Olimp”. Baza unei securități adecvate o constituie respectarea prezentei Politici. Aceasta cuprinde cerințe și reguli pentru protecția tuturor informațiilor, inclusiv confidențialitatea datelor cu caracter personal care îi sunt cunoscute despre elevi și părinți/reprezentanți legali ai acestora. Având în vedere că IPLT „Olimp” deține date de caracter a minorilor, prezenta Politică are ca scop asigurarea protecției drepturilor și libertăților fundamentale ale minorilor și familiei acestora în ceea ce privește prelucrarea datelor cu caracter personal. Persoanele împuternicite de către

operator vor asigura protecția datelor cu caracter personal prin aplicarea corespunzătoare a legislației în vigoare cu referire la protecția datelor și confidențialitatea comunicării.

IPLT „Olimp” va proteja datele cu caracter personal atât a participanților la procesul instructiv-educativ, cât și a angajaților săi.

Reglementările prezentei Politici reprezintă un standard minim pentru IPLT „Olimp”, inclusiv toți angajații IPLT „Olimp”. Pornind de la această reglementare, toți angajații IPLT „Olimp” urmează să respecte strict prevederile Politicii și regulilor interne ale IPLT „Olimp” privind protecția datelor cu caracter personal și sistemelor IT.

V.RESPONSABILITATEA RESPECTĂRII POLITICII DE SECURITATE

Responsabil de implementarea și monitorizarea respectării prevederilor politicii de securitate a datelor cu caracter personal, va fi persoana desemnată prin ordinul directorului instituției.

Persoana responsabilă (operator) desemnată, indiferent de funcțiile exercitate în cadrul monitorizării implementării/respectării prevederilor politicii de securitate, se va subordona nemijlocit directorul IPLT „Olimp” sau persoanei care îndeplinește interimatul funcției.

Persoana responsabilă (operator) de Politica de securitate a datelor cu caracter personal va defini clar responsabilitățile și procesele de management al securității datelor cu caracter personal tuturor angajaților IPLT „Olimp”.

Persoana responsabilă de Politica de securitate a datelor cu caracter personal va instrui anual persoanele implicate în procesul de prelucrare a datelor cu caracter personal în vederea îndeplinirii de către acestea a atribuțiilor funcționale și asumării responsabilităților de securitate a datelor cu caracter personal, inclusive asupra confidențialității acestora.

VI.MĂSURILE DE PROTECȚIE A DATELOR CU CARACTER PERSONAL

Protecția datelor cu caracter personal în cadrul IPLT „Olimp” (în calitate de operator de date cu caracter personal) este asigurată printr-un complex de măsuri tehnice și organizatorice de preîntâmpinare a prelucrării ilicite a datelor cu caracter personal.

Măsurile de protecție a datelor cu caracter personal, prelucrate în sistemul informațional de date cu caracter personal, se desfășurează ținând cont de necesitatea asigurării confidențialității și integrității acestora, prin protecție în formă manuală, electronică și externă.

Măsurile de protecția datelor cu caracter personal sunt asigurate în scopul:

- preîntâmpinării scurgerii informației care conține date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;
- preîntâmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în rețelele telecomunicaționale și resursele informaționale;
- neadmiterea dezvăluirii terților a informației cu accesibilitate limitată;
- eficientizarea resurselor informaționale atât pe suport de hârtie cât și cel în format electronic;
- excluderii accesului neautorizat la datele cu caracter personal prelucrate în cadrul sistemelor de evidență prin metoda implementării procedurilor de identificare și autentificare a utilizatorilor;

- preîntâmpinării acțiunilor intenționate și/sau neintenționate ale utilizatorilor interni și/sau externi, precum și ale altor deținători de date cu caracter personal, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul sistemului tehnic și de program;
- preîntâmpinarea scurgerii de informații care conțin date cu caracter personal, transmise prin canalele de legătură, prietenie, cunoștințe;
- stabilirea exactă a ordinii și procedurilor de acces la informația care conține date cu caracter personal, prelucrate în cadrul sistemelor informaționale și de evidență;

Este obligatorie respectarea unor măsuri de protecție a datelor cu caracter personal:

1. Completarea de către angajați a ACORD-ului privind prelucrarea datelor cu caracter personal al elevilor, părinților/reprezentanți legali (Anexa 1);
2. Semnarea Declarației-angajament a utilizatorului Sistemului de cartografiere a școlilor primare, gimnaziale și liceelor privind confidențialitatea datelor cu caracter personal (Anexa 2);
3. Administrarea și monitorizarea accesului online al utilizatorilor (diriginților de clasă) în sistemul de cartografiere digitale;
4. Realizarea identificării și autentificării a utilizatorului sistemelor informaționale de date cu caracter personal cu numele acestora;
5. Utilizarea programelor în cadrul sistemului informatic cu respectarea condițiilor de licențiere;
6. Utilizarea mijloacelor criptografice de protecție a informației canalului securizat VPN (rețele private virtuale) pentru transmiterea datelor cu caracter personal;
7. Păstrarea în siguranță a ordinilor, registrelor, listelor de evidență, cataloagelor școlare;
8. Corespunderea necesității asigurării securității datelor cu caracter personal contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri;
9. Restricționarea accesului în oficiile, birourile, arhivă și secretariat unde sunt amplasate sistemele informaționale de date cu caracter personal;
10. Blocarea accesului părinților/reprezentanților legali, persoanelor neautorizate la datele cu caracter personal;
11. Asigurarea perimetrului de securitate a IPLT „Olimp”, a oficiilor în care se prelucrează/stocază date cu caracter personal;
12. Prezentarea informațiilor despre date cu caracter personal strict persoanei vizate de interese;
13. Prezentarea actelor de identitate a persoanelor (părinților/reprezentanți legali) ce solicită date cu caracter personal;
14. Primire/expediere a corespondenței datelor cu caracter personal organelor ierarhic superior, direcțiilor de interese ale subiecților se realizează prin act normativ (demers, acord) de solicitare a informației, asigurând nivelul adecvat de protecție;
15. Prelucrare/stocarea datelor cu caracter personal cu utilaje foto/video neautorizate este interzis;
16. Folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare pe teritoriul

instituției se realizează cu permisiunea specială a conducerii, în vederea evitării riscurilor speciale pentru drepturile și liberățile minorilor.

VII.DEZVĂLUIREA DATELOR CU CARACTER PERSONAL

1. Dezvăluirea formatului electronic al datelor cu caracter personal conținute în sistemele de evidență, dosarele personale, ale elevilor, cataloagele școlare, actele de studii, prin rețele comunicaționale ori pe alt suport digital de stocare și păstrare, urmează a fi asigurată criptarea acestei informații sau examinarea posibilității utilizării unei conexiuni bilaterale prin canal securizat VPN. Accesul fără fir la sistemele de evidență a datelor cu caracter personal este permis doar utilizatorilor autorizați. Fiecare caz de solicitare a dezvăluirii prin transmitere a datelor cu caracter personal pe cale electronică va fi examinat separat, reieșind din posibilitățile tehnice asigurate de destinatar și operator, precum și în corespundere cu măsurile organizatorice și tehnice implementate de părți. În cazul în care rețelele comunicaționale prezintă riscuri pentru confidențialitatea și securitatea datelor cu caracter personal, vor fi utilizate metode tradiționale de transmitere (*expediere poștală cu aviz recomandat, înmânarea personală, etc.*).

2. Dezvăluirea prin transmitere a datelor cu caracter personal care vizează elevii/părinții/lucrători ai instituției prin rețele comunicaționale ce nu corespund Cerințelor, (*spre exemplu: expedierea informației prin intermediul e-mail-urilor personale de tipul @gmail.com, @mail.ru, @yahoo.com, etc.*) sunt interzise.

3. Sunt interzise operațiunile de dezvăluire a datelor cu caracter personal între și alte entități care sunt amplasate geografic în stânga Nistrului care refuză să se supună juridic legislației Republicii Moldova, reieșind din considerentul că la moment nu există posibilitatea exercitării unui control efectiv asupra acestei părți teritoriale, inclusiv în partea ce ține de conformitatea prelucrării datelor cu caracter personal prevederilor Legii privind protecția datelor cu caracter personal.

4. Procedura dezvăluirii prin transmitere a datelor cu caracter personal stocate pe suport de hârtie și/sau suport digital, peste hotarele Republicii Moldova, urmează a fi reglementată prin act normativ instituțional/acord bilateral luându-se în considerare necesitatea asigurării unui nivel adecvat de protecție a datelor cu caracter personal.

5. Transmiterea transfrontalieră a datelor cu caracter personal este efectuată în strictă corespundere cu prevederile art. 32 al Legii privind protecția datelor cu caracter personal, cu anunțarea structurilor ierarhic superior.

6. Volumul și categoriile datelor cu caracter personal colectate în scopul ținerii evidenței IPLT „Olimp”, este limitat la strictul necesar pentru realizarea scopurilor declarate.

7. Acces la sistemele informaționale gestionate în cadrul IPLT „Olimp”, din partea Procuraturii General (*după caz procuraturile teritoriale/specializate*), Ministerului Afacerilor Interne, Centrului Național Anticorupție etc., va fi permis doar în cazul în care solicitarea va corespunde prevederilor art. 15 și art. 212 Cod de procedură penală.

Se explică că în conformitate cu prevederile art. 157 Cod de procedură penală, documentele în orice formă (*scrisă, audio, video, electronică etc.*) care provin de la persoane oficiale fizice sau juridice dacă în ele sunt expuse ori adevărate circumstanțe care au importanță pentru cauză, (*inclusiv informația stocată în auditul sistemelor*

informaționale și de evidență), pot fi solicitate printr-un demers al organului de urmărire penală în cadrul urmăririi penale sau în procesul judecării cauzei. În acest caz, însă, urmează a fi respectate prevederile art.214 Cod de procedură penală, care stipulează că în cursul procesului penal nu pot fi administrate, utilizate și răspândite fără necesitate informație oficială cu accesibilitate limitată. Persoanele cărora organul de urmărire penală sau instanța le solicită să comunice sau să prezinte informație oficială cu accesibilitate limitată (*inclusiv operatorii de date cu caracter personal*) au dreptul să se convingă de faptul că aceste date se colectează pentru procesul penal respectiv, iar în caz contrar să refuze de a comunica sau de a prezenta date. Persoanele cărora organul de urmărire penală sau instanța le solicită să comunice sau să prezinte informație oficială cu accesibilitate limitată au dreptul să primească în prealabil de la persoana care solicită informații o explicație în scris care ar confirma necesitatea furnizării datelor menționate.

Urmează a ține cont de faptul că în conformitate cu prevederile art.8 al Legii privind accesul la informație, datele cu caracter personal fac parte din categoria informației oficiale cu accesibilitate limitată, accesul la care se realizează în conformitate cu prevederile legislației privind protecția datelor cu caracter personal.

În cazul în care, avocatul sau persoana împuternicită solicită să ia cunoștință cu fișa personală a persoanei, aceștia urmează a fi informați în scris despre obligațiile ce le revin în conformitate cu prevederile art. 15 Cod de procedură penală, art. 29 și 30 ale Legii privind protecția datelor cu caracter personal, inclusiv despre răspunderea prevăzută de art. 74¹ Cod contravențional.

VIII.DREPTURILE SUBIECȚILOR LA DATE CU CARACTER PERSONAL

Subiecții datelor cu caracter personal (părinții/reprezentanți legali) au dreptul să dețină informațiile respective:

- Scopurile prelucrării datelor cu caracter personal;
- Corectitudinea întocmirii actelor;
- Destinatarii datelor cu caracter personal;
- Actele întocmite și verificarea corectitudinii;
- Datele despre rezultatele instruirii copiilor săi (notele/calificativele).

În acest sens, persoanele responsabile (diriginți de clasă, cadre didactice, secretarul) de prelucrarea datelor cu caracter personal, vor asigura accesul persoanei doar la datele cu caracter personal care-o vizează nemijlocit, fiind exclusă posibilitatea consultării datelor cu caracter personal ce vizează alți subiecți.

IX.STOCAREA, PĂSTRAREA ȘI DISTRUGEREA DATELOR CU CARACTER PERSONAL

1. Stocarea și păstrarea datelor cu caracter personal consemnate în dosarele elevilor și alte documente, sunt efectuate în strict conformitate cu prevederile legislației învățământului; MECC și DGETS mun.Chișinău.

2. Accesul în spațiile/perimetrul unde sunt amplasate sistemele informaționale și de evidență a datelor cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară conform politicii de securitate instituționale /regulamentelor aprobate.

3. Stocarea și păstrarea formatului electronic al datelor cu caracter personal, structurate în sisteme de evidență, în computere care sunt conectate la internet, nu sunt echipate cu mijloace de protecție speciale tehnice și de program și nu au instalate programe licențiate, programe antivirus, sisteme de control al securității soft-ului, de asigurare a efectuării periodice a copiilor de siguranță și de efectuare a auditului - este interzisă.

4. Introducerea în perimetrul de securitate instituțional și utilizarea calculatoarelor personale ori a purtătorilor de informații în scopuri de serviciu este interzisă. Mai mult, accesul la computerele din dotare sunt protejate/restricționate prin crearea profilurilor de utilizatori, iar drepturile de administrator sunt încredințate doar persoanei responsabile pentru implementarea politicii de securitate desemnate din cadrul IPLT „Olimp”.

4. Stocarea datelor cu caracter personal pe suport magnetic, optic, laser, de hârtie sau alt suport al informației, pe care se creează, se fixează, se transmite, se recepționează, se păstrează sau, în alt mod, se utilizează documentul și care permite reproducerea acestuia, este asigurat prin plasarea acestora în safeuri sau dulapuri metalice care se încuie. Scoaterea, fără autorizare, a purtătorilor de date cu caracter personal din perimetrul de securitate al operatorului este interzisă.

X.AUDITUL SISTEMELOR INFORMAȚIONALE GESTIONATE

1. Se efectuează înregistrarea tentativelor de intrare/ieșire a utilizatorului în sistem, conform următorilor parametri:

- data și timpul tentativei intrării/ieșirii;
- ID-ul utilizatorului;
- rezultatul tentativei de intrare/ieșire - pozitivă sau negativă.

2. Se efectuează înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:

- data și timpul tentativei de obținere a accesului (executare a operațiunii),
- denumirea (identificatorul) aplicației sau procesului, o ID-ul utilizatorului,
- specificațiile resursei protejate (identificator, nume logic, nume fișier, număr etc.),
- tipul operațiunii solicitate (citire, înregistrare, ștergere etc.),
- rezultatul tentativei de obținere a accesului (executare a operațiunii) — •pozitivă sau negativă.

3. Este efectuată înregistrarea modificărilor drepturilor de acces (competențelor) utilizatorului și statutului obiectelor de acces, conform următorilor parametri:

- data și timpul modificării competențelor,
- ID-ul administratorului care a efectuat modificările,
- ID-ul utilizatorului și competențele acestuia sau specificarea obiectelor de acces și statutul nou al acestora.

4. Se efectuează înregistrarea ieșirii din sistem a informației care conține date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecților și statutul obiectelor de acces, conform următorilor parametri:

- data și timpul eliberării,
- denumirea informației și căile de acces la aceasta,

- specificarea echipamentului (dispozitivului) care a eliberat informația (numele logic),
- ID-ul utilizatorului, care a solicitat informația.

XI.GESTIONAREA INCIDENTELOR DE SECURITATE

1. Personalul care asigură exploatarea sistemelor informaționale de date cu caracter personal trece, minimum o dată în an, instruirea referitor la responsabilitățile și obligațiile în cazul executării acțiunilor de gestionare și reacționare la incidentele de securitate.
2. Personalul IPLT „Olimp” informează neîntârziat conducerea despre incidentele care încalcă securitatea sistemelor informaționale de date cu caracter personal.
3. Prelucrarea incidentelor include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor și restabilirea securității.
4. Până la 31 ianuarie a fiecărui an, operatorul de date cu caracter personal informează în scris Centrul Național pentru Protecția Datelor cu Caracter Personal despre incidentele de securitate constatate.
5. În cazul producerii incidentelor de securitate în cadrul IPLT „Olimp”, persoana responsabilă va întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia și va înlătura cauzele incidentului de securitate cu informarea, în termen de 72 ore din momentul producerii incidentului de securitate, a Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova.
6. În cadrul controalelor efectuate de Centrul Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova i se va oferi suportul necesar și asigurat accesul la informațiile necesare relevante obiectului controlului.

XII.MARCAREA DOCUMENTELOR

Toată informația care se intenționează a fi dezvăluită, si care conține date cu caracter personal, urmează a fi marcată prin includerea numărului de înregistrare din Registrul de evidență al operatorilor de date cu caracter personal.

Model

Documentul conține date cu caracter personal, prelucrate în cadrul sistemului de evidență nr. __, înregistrat în Registrul de evidență al operatorilor de date cu caracter personal www.registru.datepersonale.md. Prelucrarea ulterioară a acestor date poate fi efectuată numai în condițiile prevăzute de Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal.

XIII.RENSPONSABILITATEA LEGALĂ PENTRU ASIGURAREA DATELOR CU CARACTER PERSONAL

Reponsabilul de date cu caracter personal (administrația instituției, cadre didactice, diriginți de clasă, personal tehnic), personae împuternicite de către responsabil (administrator) , persoanele terțe după caz, semnatari/ împuterniciți, pentru nerespectarea dispozițiilor Politicii de securitate poartă răspundere civilă (Cod Civil), contravențională (art.74¹ Cod Contravențional) și penală (art. 177, 178, 180 Cod Penal).

XIV.DISPOZIȚII FINALE

Prezenta Politica de securitate este aprobată la Consiliul de administrație și Notificată de Centrul Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova. Politica de securitate este adusă la cunoștința angajaților contra semnăturii.

ACORD
PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL
ALE SALARIAȚILOR

Subsemnatul _____,

(numele, prenumele)

IDNP |_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|

Angajat al _____

(denumirea instituției, adresa, telefon)

Funcția _____

(denumirea funcției/postului ocupat)

prin acest Acord îmi exprim consimțământul ca administrația IPLT „Olimp” să prelucreze datele mele cu caracter personal, care sunt oferite de către mine, în legătura cu apariția raporturilor de serviciu/muncă, precum și să colecteze și să prelucreze datele mele pe durata raporturilor de serviciu/muncă și să asigure limitarea accesului persoanelor neautorizate în spațiile destinate exclusive salariaților, precum și la locul de muncă.

<i>Nume, prenume</i>	<i>Semnătura</i>
	<i>Data</i>

Confirm că am fost informat(ă) cu prevederile „Politicii de securitate privind protecția datelor cu caracter personal în sistemele de evidență” ale IPLT „Olimp” și că mi s-a adus la cunoștință cu prevederile Legii nr.133 din 8 iulie 2011 privind protecția (confidențialitatea) datelor cu caracter personal al beneficiarilor și titularilor procesului instructiv în instituție de învățământ și responsabilitățile mele privind prelucrarea datelor cu caracter personal și mi s-a adus la cunoștință drepturile mele prevăzute în aceeași lege.

<i>Nume, prenume</i>	<i>Semnătura</i>
	<i>Data</i>

Declarație – angajament a utilizatorului
Sistemului de cartografiere a școlilor primare, gimnaziilor și liceelor
privind confidențialitatea datelor cu caracter personal (SIME)

Subsemnatul _____,

(numele, prenumele)

IDNP |_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|

Angajat al _____

(denumirea instituției, adresa, telefon)

Funcția _____

(denumirea funcției/postului ocupat)

Locul desfășurării activității _____

(denumirea raionului/municipiului/UTA, localității și adresa sediului instituției)

În conformitate cu prevederile Legii nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal și a Hotărârii Guvernului nr. 1123 din 14 decembrie 2010 „Privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal”, mă oblig să respect drepturile și libertățile fundamentale ale persoanelor cu privire la prelucrarea, confidențialitatea și securitatea datelor cu caracter personal.

Conștientizez că în cazul divulgării datelor cu caracter personal voi purta răspundere în conformitate cu legislația în vigoare.

<i>Nume, prenume</i>	<i>Semnătura</i>
	<i>Data</i>