

POLITICA DE PRELUCRARE ŞI PROTECŢIE A DATELOR CU CARACTER PERSONAL

DOCUMENT

Privind măsurile de protecţie a persoanelor ale căror date cu caracter personal sunt prelucrate de către ***Şcoala Gimnaziala Nr. 2 Fundeni-Dobroesti***

CUPRINS

Titlul I. Scopul Politicii 4
Titlul II. Domeniul de aplicare..... 4
Titlul III. Referinţe normative..... 5
Titlul IV. Descrierea procedurilor..... 6
Secţiunea I. Prelucrarea datelor cu caracter personal..... 7
Secţiunea II. Solicitarea accesului la datele cu caracter personal.....24
Secţiunea III. Categorii de incidente şi soluţionarea acestora.....26
Secţiunea IV. Cerinţele minime de securitate 28

Titlul V. DISPOZIŢII FINALE 35

1. Lista responsabililor cu elaborarea, verificarea, aprobarea procedurii

Nr. Crt	Elemente privind resp. operaţiune	Numele şi prenumele	Funcţia	Data	Semnătura
	1	2	3	4	5
1.	Elaborat	CARMEN DONACHE	DPO	03.05.2023	
2.	Verificat	PREDA NICUŞOR	PROFESOR	03.05.2023	
3.	Avizat/Aprobat	PROF.STUPINEANU CLAUDIA	Director		

Titlul III. Referinţe normative

Art. 5. În stabilirea Procedurii s-a făcut apel la următoarele referinţe normative:

Legea educaţiei naţionale nr.1/ 2011, cu modificările şi completările ulterioare;

Regulamentul (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de;

Legea nr. 544/ 2001 privind liberul acces la informaţiile de interes public;

Legea nr. 16/ 1996 a Arhivelor Naţionale (cu modificările ulterioare);

OMEN nr. 5.447/31.08.2020 privind aprobarea Regulamentului de organizare şi funcţionare a unităţilor de învăţământ preuniversitar;

Ordinul nr. 5545/09.2020 pentru aprobarea Metodologiei-cadru privind desfăşurarea activităţilor didactice prin intermediul tehnologiei şi al internetului, precum şi pentru prelucrarea datelor cu caracter personal;

Ordinul ministrului educaţiei şi cercetării şi al ministrului sănătăţii nr. 5.487/1.494/2020 privind aprobarea măsurilor de organizare a activităţii în cadrul unităţilor/instituţiilor de învăţământ în condiţii de siguranţă epidemiologică pentru prevenirea îmbolnăvirilor cu virusul SARS-CoV-2;

OMEN nr. 4619/ 2014 pentru aprobarea Metodologiei – cadru de organizare şi funcţionare a Consiliului de Administraţie din unităţile de învăţământ preuniversitar, cu modificările si conpletările ulterioare;

Regulamentul Intern al Scolii Gimnaziale Nr. 2

Titlul IV. Descrierea procedurii-definiţii:

(1) **Date cu caracter personal** – înseamnă orice informaţii privind o persoană fizică identificată sau identificabilă („persoana vizată"); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identităţii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

(2) **Prelucrarea datelor cu caracter personal** – înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;

(3) **Consimțământul persoanei vizate** – înseamnă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;

(4) **Stocarea** – păstrarea pe orice fel de suport a datelor cu caracter personal culese;

(5) **Operator** – înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern;

(6) **Persoană împuternicită de operator** – înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

(7) **Parte Terță** – înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;

(8) **Destinatar** – înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Cu toate acestea, autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de

către autoritățile publice respective respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării;

(9) **Date anonime** – date care, datorită originii sau modalității specifice de prelucrare, nu pot fi asociate cu o persoană identificată sau identificabilă;

(10) **Pseudonimizare** – înseamnă prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;

(11) **Sistem de evidență a datelor cu caracter personal** – înseamnă orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcționale sau geografice;

Secțiunea I. Modul de operare/aplicare

Art. 6. Principii generale

(1) Prelucrarea datelor cu caracter personal se realizează cu respectarea regulilor generale și speciale prevăzute de Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), a deciziilor cu caracter normativ emise de Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, denumită în continuare Autoritatea națională și a procedurilor proprii elaborate de Școala Gimnaziala Nr. 2.

(2) Datele cu caracter personal sunt colectate și prelucrate în cadrul documentelor (pe suport hârtie) prin sistemul de evidență manuală, în format electronic prin sistemul de evidență automat/informatic sau prin intermediul sistemului de supraveghere video.

(3) Școala Gimnaziala Nr. 2 și structurile sale stabilește ca principală responsabilitate prelucrarea legală și corectă a datelor cu caracter personal, în

considerarea respectării drepturilor și libertăților fundamentale ale persoanei, iar regulile instituite prin intermediul prezentelor proceduri trebuie să asigure confidențialitatea acestei categorii de informații.

(4) Personalul angajat la Școlii Gimnaziala Nr. 2 și structurile sale prelucrează datele cu caracter personal cu aplicarea principiilor legalității, necesității, confidențialității și proporționalității.

(5) Școala Gimnaziala Nr. 2 și structurile sale promovează principiile prelucrării datelor cu caracter personal, prevăzute în art. 5 din Regulamentul 679/2016, potrivit cărora datele cu caracter personal trebuie să fie:

a) prelucrate în mod legal, echitabil și transparent față de persoana vizată ("legalitate, echitate și transparență");
b) colectate în scopuri determinate, explicite și legitime și fără a fi prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile inițiale, în conformitate cu articolul 89 alineatul (1) („limitări legate de scop");
c) adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate („reducerea la minimum a datelor");
d) exacte și, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere („exactitate");
e) păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1), sub rezerva punerii în aplicare a măsurilor de ordin tehnic și organizatoric adecvate

prevăzute în prezentul regulament în vederea garantării drepturilor și libertăților persoanei vizate („limitări legate de stocare");

f) prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare („integritate și confidențialitate").

(6) Operatorul este responsabil de respectarea acestor principii și poate demonstra această respectare ("responsabilitate").

(7) Școala Gimnaziala Nr. 2 și structurile sale, prin intermediul regulilor implementate la nivelul societății, promovează principiul respectării drepturilor prevăzute de Regulamentul 679/2016, respectiv, dreptul la informare, dreptul de acces, dreptul la rectificare și dreptul la ștergerea datelor (dreptul de a fi uitat), dreptul la restricționarea prelucrării, dreptul la portabilitatea datelor, dreptul de opoziție, dreptul de a nu fi supus unui proces decizional individual automatizat, inclusiv crearea de profiluri, dreptul de a se adresa cu o plângere la autoritatea de supraveghere și dreptul de a se adresa justiției.

Art. 7 Conform Regulamentului (UE) pentru protecția datelor 2016/679 (GDPR), este necesar ca școala să aibă o politică privind protecția datelor cu caracter personal inclusiv pentru securitatea în mediul educațional virtual, care să fie accesibilă părinților și elevilor, în scopul informării lor.

(1). În acest scop conducerea Școala Gimnaziala Nr. 2 și structurile sale, publică pe site-ul școlii și prin afișare la sediu următoarele informații:

- identitatea și datele de contact ale unității de învățământ și, după caz, ale reprezentantului acesteia;
- scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării;
- destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
- perioada pentru care vor fi stocate datele cu caracter personal, drepturile persoanelor vizate.

Art.8 Obligaţia de informare se regăseşte în art. 13 din Regulamentul general privind protecţia datelor nr. 679/2016, iar nerespectarea de către operator poate fi sancţionată.

(1). Categorii de informaţii colectate şi protejate, inclusiv în mediul educaţional virtual

Şcoala Gimnaziala Nr. 2 şi structurile sale, prelucrează datele cu caracter personal (CNP, date din cartea de identitate, stare de sănătate, adresă, email, număr telefon, etc.) a următoarelor categorii de persoane fizice, în funcţie de scopul prevăzut în prezenta procedură:

a) Elevii, părinţi ai acestora, reprezentanţi legali ai acestora, alţi membri ai familiei;

b) personal didactic, personal didactic auxiliar şi personal nedidactic aflat în relaţii contractuale cu Şcoala Gimnaziala Nr. 2, candidaţi la concursurile de ocupare a posturilor didactice, didactice auxiliare şi administrative/ nedidactice;

c) Orice persoană fizică sau juridică ce are raporturi de natură comercială sau contractuală cu Şcoala Gimnaziala Nr. 2 şi structurile sale.

În contextul protecţiei datelor cu caracter personal ale elevilor, prelucrarea trebuie să respecte şi principiul interesului superior al copilului.

(2). În ceea ce priveşte datele cu caracter personal utilizate în mediul educaţional virtual, categoriile de date care trebuie prelucrate cu respectarea principiilor legate de prelucrarea datelor cu caracter personal sunt:

a) numele şi prenumele preşcolarilor/elevilor, numele şi prenumele cadrelor didactice care utilizează aplicaţia/platforma educaţională informatică;

b) imaginea, vocea participanţilor, după caz;

c) mesajele, videoclipurile, fişierele expediate sau orice alte materiale care conţin date prelucrate prin utilizarea aplicaţiei/platformei educaţionale informatice;

d) rezultatele evaluării;

e) datele de conectare la aplicaţia/platforma educaţională utilizată pentru participare la cursurile online: nume de utilizator şi parolă de acces.

(3) În scopul îndeplinirii atribuţiilor prevăzute de legislaţia în vigoare a activităţii didactice Şcoala Gimnaziala Nr. 2 şi structurile sale, colectează şi prelucrează următoarele categorii de date cu caracter personal:

a) numele şi prenumele
b) nume anterior
c) prenumele tatălui şi prenumele mamei
d) sexul
e) data şi locul naşterii
f) cetăţenia
g) codul numeric personal
h) seria şi numărul actului de identitate
i) semnătura
j) starea civilă
k) date biometrice
l) telefon/fax
m) reşedinţa/domiciliul
n) profesia
o) loc de muncă
p) imagine
q) înregistrări video
r) alte date necesare derulării activităţilor specifice

(4) Prelucrarea datelor cu caracter personal se realizează după obţinerea consimţământului persoanei vizate, înscris în formularul tipizat de consimţământ.

(3). Scopul şi motivaţia colectării şi prelucrării datelor cu caracter personal

Şcoala Gimnaziala Nr. 2 şi structurile sale are obligaţia de a administra în condiţii de siguranţă şi numai pentru scopurile specificate, datele personale care îi sunt furnizate despre categoriile de persoane fizice prevăzute mai sus.
Scopul colectării datelor este:

a) Pentru elevi şi aparţinători: prestări de servicii ale Şcolii Gimnaziala Nr. 2 şi structurile sale, pentru realizarea obiectului de activitate principal, respectiv: educaţie şi cultură, asigurarea dreptului la învăţătură.
b) Pentru alte persoane: pentru scopuri de natură comercială.
c) Pentru angajaţii unităţii: derularea raporturilor de muncă.

(4)Reguli specifice ale prelucrării de date cu caracter personal

(1) Şcoala Gimnaziala Nr. 2 şi structurile sale, prelucrează date cu caracter personal, potrivit legii, în următoarele scopuri:

I. - specifice domeniului de activitate:

a) - pentru întocmirea documentaţiei de înregistrare ca elev în cadrul unităţii de învăţământ,

b)- pentru sprijinirea procesului de recepţionare a serviciilor şi derularea relaţiilor cu toţi colaboratorii şi părinţi ai elevilor;

c) -constituirea şi gestionarea bazei de date,

d)- procesarea datelor pentru recepţionarea serviciilor;

e)- colectarea datelor prin intermediul formularului de contact, prin e-mail, telefon si/sau fax referitoare la înscrierea copiilor în cadrul şcolii sau solicitarea diverselor informaţii;

f)- executarea unei operaţiuni de plată;

g)- prelucrarea oricăror alte solicitări primite direct sau online, inclusiv formularea răspunsurilor la solicitări;

h)- încheierea şi executarea de contracte;

i)- administrarea şi întreţinerea website-ului;

II. -în scopuri administrative:

a)- activităţi de recrutare şi selecţie de candidaţi calificaţi, capabili sa ocupe posturile vacante din cadrul instituţiei;

b)- promovarea unor acţiuni şi evenimente;

c)- pentru analize interne destinate îmbunătăţirii serviciilor publice;

d)- îndeplinirea altor obligaţiilor legale specifice domeniului de activitate.

Prelucrarea, de către Şcoala Gimnaziala Nr. 2 şi structurile sale, a datelor cu caracter personal ale participanţilor la activităţile desfăşurate prin intermediul tehnologiei şi al internetului se realizează în vederea îndeplinirii obligaţiei legale care revine unităţii de învăţământ de asigurare a dreptului la învăţătură, prin garantarea accesului şi a desfăşurării efective a procesului educaţional în cazul în care procesul educaţional nu se poate derula faţă în faţă.

Datele cu caracter personal prevăzute mai sus sunt prelucrate exclusiv în scopul derulării activităţii didactice.

Orice prelucrare a datelor cu caracter personal efectuată de către unitate în afara acestui scop, constituie o încălcare a prevederilor legale.

(4). Obținerea consimțământului privind prelucrarea datelor cu caracter personal

Școala trebuie să obțină consimțământul părinților / reprezentanților legali / elevilor peste 18 ani / angajaților sau potențialilor angajați, persoanelor cu care școala are relații contractuale, pentru prelucrarea datelor cu caracter personal, inclusiv pentru datele utilizate în mediul educațional virtual.

Sunt stabilite formulare pentru consimțământ:

- Formular de consimțământ privind prelucrarea datelor cu caracter personal pentru părinti și elevi (care sunt furnizate părintilor, reprezentaților legali)-**anexa nr.1**
- Acord privind prelucrarea datelor cu caracter personal, utilizate pentru personalul angajat sau pentru cei care doresc să se angajeze- **anexa nr.2**

Consimțământul reprezentatului legal al copilului este necesar și pentru fotografierea elevilor, altfel nefiind permisă publicarea fotografiilor de către unitatea de învățământ (acceptul se regăseste în formularul de consimtământ).

Școala Gimnaziala Nr. 2 și structurile sale, poate să nu solicite consimțământul prealabil al părinților atunci când fotografiile nu permit identificarea facilă a elevilor.

Totuși, în asemenea cazuri, rămâne obligatorie informarea elevilor, părinților/reprezentanților legali că se va face o fotografie și modul în care va fi aceasta utilizată, fiindu-le oferită posibilitatea de a refuza să facă parte din fotografie.

(5). Utilizatorii datelor au următoarele obligații specifice:

a) să cunoască și să aplice prevederile actelor normative din domeniul prelucrării datelor cu caracter personal precum și ale prezentei proceduri;

b) să păstreze confidențialitatea datelor prelucrate, a contului de utilizator, a parolei/ codului de acces la sistemele informatice/ baze de date prin care sunt gestionate date cu caracter personal;

c) să respecte măsurile de securitate, precum și celelalte reguli stabilite de unitate;

d) să informeze de îndată conducerea operatorului despre împrejurări de natură a conduce la o diseminare neautorizată de date cu caracter personal sau despre o situaţie în care au fost accesate/ prelucrate date cu caracter personal prin încălcarea normelor legale, despre care a luat la cunoştinţă.

(6). Participanții la activitățile de învățare desfășurate prin intermediul tehnologiei și al internetului au următoarele obligații:

a) răspund pentru toate mesajele, videoclipurile, fișierele expediate sau pentru orice alte materiale prelucrate prin utilizarea aplicației/platformei educaționale informatice;

b) de a utiliza aplicația/platforma educațională informatică doar în conformitate cu prevederile legale;

c) de a nu înregistra, disemina, folosi informații, care conțin date cu caracter personal, în alt mod care este în afara scopului prelucrării acestor date.

Art. 9. Prelucrarea datelor personale

(1) Școala Gimnaziala Nr. 2 şi structurile sale prelucrează date cu caracter personal în scopuri de învățământ, organizare, gestiune economico-financiară şi administrativă privind proprii angajaţi şi membrii de familie ai acestora, în cadrul activităţii de management resurse umane, asigurarea asistenţei medicale sau pentru desfăşurarea unor activităţi cultural-artistice, ori sportive.

(2)Scoala Gimnaziala Nr. 2 şi structurile sale care prelucrează date cu caracter personal cu ocazia organizării unor concursuri sau examene, stabilesc condiţiile concrete de asigurare a securităţii prelucrărilor, precum şi de informare a persoanelor vizate privind drepturile acestora.

Datele cu caracter personal astfel prelucrate se arhivează conform legii după realizarea scopului în care au fost prelucrate. Stocarea acestor date pentru o perioadă mai mare decât cea necesară realizării scopului se poate efectua numai pentru interes statistic, după ce au fost transformate în date anonime.

(3)Supravegherea prin mijloace audio şi/ sau video, fixe sau mobile, a unor spaţii publice perimetrale ori adiacente propriilor sedii, precum şi a spaţiilor interioare

ale acestora constituie o prelucrare a datelor cu caracter personal doar dacă aceasta este însoţită de un sistem de stocare a datelor care permite identificarea ulterioară, prin orice mijloace, a persoanei vizate.

(4)În acest caz este obligatorie avertizarea personalului propriu şi a publicului privind existenţa sistemului de supraveghere, precum şi informarea acestuia privind identitatea operatorului, scopul prelucrării, categoriile de date prelucrate, destinatarii datelor sau alte date suplimentare, după caz, conform legii. Instalarea acestor mijloace se realizează astfel încât, pe cât posibil, să nu fie vizualizat interiorul altor imobile sau căile de acces la acestea, aflate în zona adiacentă echipamentelor de supraveghere.

(5)Prelucrarea datelor cu caracter personal se poate realiza prin mijloace automate sau neautomate în cadrul unor operaţiuni ori seturi de operaţiuni, fără a fi limitate la acestea, după cum urmează:

a) colectarea - strângerea, adunarea ori primirea datelor cu caracter personal prin orice mijloace legale şi din orice sursă;

b) înregistrarea - consemnarea datelor cu caracter personal într-un sistem de evidenţă automat ori neautomat, care poate fi registru, fişier automat, bază de date sau orice altă formă de evidenţă organizată, structurată ori ad-hoc sau într-un text, înşiruire de date ori document, indiferent de modalitatea în care se înscriu datele;

c) organizarea - ordonarea, structurarea sau sistematizarea datelor cu caracter personal, conform unor criterii prestabilite, potrivit atribuţiilor legale ale operatorului, în scopul eficientizării/ optimizării activităţilor de prelucrare a acestora;

d) stocarea - păstrarea pe orice fel de suport a datelor cu caracter personal culese, inclusiv prin efectuarea copiilor de siguranţă;

e) adaptarea - transformarea datelor cu caracter personal colectate iniţial, conform criteriilor prestabilite şi scopurilor pentru care au fost colectate;

f) modificarea - actualizarea, completarea, schimbarea, corectarea ori refacerea datelor cu caracter personal, în scopul menţinerii caracteristicilor de exactitate, realitate, actualitate;

g) extragerea - scoaterea unei părţi din categoria specifică de date cu caracter personal, în scopul utilizării acesteia, separat şi distinct de prelucrarea iniţială;

h) consultarea - examinarea, vizualizarea, interogarea ori cercetarea datelor cu caracter personal, fără a fi limitate la acestea, în scopul efectuării unei operaţiuni sau set de operaţiuni de prelucrare ulterioară;

i) utilizarea - folosirea datelor cu caracter personal, în tot sau în parte, de către şi în interiorul operatorului, împuterniciţilor operatorului ori destinatarului, după caz, inclusiv prin tipărire, copiere, multiplicare, scanare sau orice alte procedee similare;

j) dezvăluirea - a face disponibile date cu caracter personal către terţi prin comunicare, transmitere, diseminare sau în orice alt mod;

k) alăturarea - adăugarea, alipirea sau anexarea unor date cu caracter personal la cele deja existente, pe care nu le modifică;

l) combinarea - îmbinarea, unirea sau asamblarea unor date cu caracter personal separate iniţial, într-o formă nouă, pe baza unor criterii prestabilite, pentru scopuri anume determinate;

m) blocarea - întreruperea prelucrării datelor cu caracter personal;

n) ştergerea - eliminarea sau înlăturarea, în tot sau în parte, a datelor cu caracter personal din evidenţe sau înregistrări, prin împlinirea termenului de păstrare, la atingerea scopului pentru care au fost introduse, caducitatea, inexistenţa, inexactitatea;

o) transformarea - operaţiunea efectuată asupra datelor cu caracter personal având ca scop anonimizarea ori utilizarea acestora în scopuri exclusiv statistice;

p) distrugerea - aducerea la stare de neîntrebuinţare, în condiţiile legii, definitivă şi irecuperabilă, prin mijloace mecanice sau termice, a suportului fizic pe care au fost prelucrate date cu caracter personal.

Stocarea datelor cu caracter personal se realizează în condiţiile stabilite prin actul normativ care reglementează scopul prelucrării şi potrivit regulilor generale de arhivare a documentelor.

Art. 10.Măsuri tehnice privind protejarea datelor cu caracter personal

(1) Scoala Gimnaziala Nr. 2 şi structurile sale, în calitate de operator de date cu caracter personal, instituie măsuri tehnice și organizatorice privind protejarea și păstrarea datelor cu caracter personal care să vizeze:

a) securitatea în mediul online;

b) asigurarea confidențialității datelor;
c) preîntâmpinarea riscului pierderii de date;
d) împiedicarea modificării datelor cu caracter personal;
e) interzicerea accesului neautorizat la datele cu caracter personal.

Ca măsură de protecție a datelor cu caracter personal, prelucrate cu ocazia utilizării aplicațiilor/platformelor educaționale informatice, se interzice înregistrarea activităților desfășurate online.

La nivelul școlii trebuie să existe o cartografiere a documentelor care conțin date cu caracter personal **(Registru de evidenta a datelor cu caracter personal)- anexa nr 4**

Pentru aceste documente se stabilește cine le colectează și sub ce formă, cine le prelucrează, cine le utilizează, unde se transmit și măsurile de protecție pentru fiecare document / baza de date care conține aceste date.

Toate documentele care conţin date cu caracter personal se înregistrează şi urmează regulile de păstrare, procesare, multiplicare, transport, transmitere, distrugere şi arhivare stabilite prin Legea Arhivelor nationale şi prin proceduri interne.

Cu ocazia proiectării, întreţinerii, actualizării aplicaţiilor de gestiune a bazelor de date, se interzice accesul programatorilor/ personalului de întreţinere a sistemelor informatice la orice fel de date cu caracter personal deţinute/ create/ accesate de personalul din structura respectivă. În aceste situaţii, se pun la dispoziţia programatorilor/ personalului de întreţinere numai date anonime.

Pentru cazuri excepţionale, numai pe durata intervenţiei şi circumstanţiat limitativ la datele strict necesare, persoanele care asigură suportul tehnic pot avea acces la datele cu caracter personal numai în prezenţa unui utilizator desemnat de director, în această situaţie, răspunderea pentru păstrarea confidenţialităţii datelor aparţine persoanelor în cauză, sens în care trebuie să semneze un angajament de confidenţialitate.

Operaţiunile de colectare, introducere, modificare şi actualizare a datelor cu caracter personal se fac numai de personalul anume desemnat de către director.

Bazele de date cu caracter personal deţinute/ create şi programele folosite de operatori sunt salvate, prin copii de siguranţă, la un interval de timp stabilit, în

funcţie de mărimea, volumul şi importanţa acestor baze de date, care nu poate depăşi 6 luni.
Directorul desemnează utilizatori care trebuie să aibă ca atribuţie de serviciu şi executarea copiilor de siguranţă ale bazelor de date deţinute/ create şi ale programelor folosite.
În cazul în care nu se poate restricţiona accesul în aceste încăperi, documentele se securizează în dulapuri/ fişete metalice închise cu chei.
Aplicaţiile informatice care gestionează date cu caracter personal trebuie prevăzute cu facilitatea închiderii automate a sesiunii de lucru dacă utilizatorul nu acţionează asupra datelor afişate pe ecran o perioadă de timp de până la 5 minute, stabilită în funcţie de operaţiile care trebuie executate.

Art.11. Legalitatea prelucrării datelor cu caracter personal

(1)Prelucrarea este legală numai dacă şi în măsura în care se aplică cel puţin una dintre următoarele condiţii:

a) persoana vizată şi-a dat consimţământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;

b) prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;

c) prelucrarea este necesară în vederea îndeplinirii unei obligaţii legale care îi revine unităţii de învăţământ;

d) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;

e) prelucrarea este necesară pentru îndeplinirea unei sarcini care serveşte unui interes public sau care rezultă din exercitarea autorităţii publice cu care este învestită unitatea de învăţământ

(2)Persoanele vizate beneficiază de următoarele drepturi referitoare la propriile date cu caracter personal:

a) Dreptul de opoziţie
b) Dreptul de acces la date
c) Dreptul de intervenţie asupra datelor

d) Dreptul la informare – poți solicita informații privind activitățile de prelucrare a datelor personale;
e) Dreptul la rectificare – poți rectifica datele personale inexacte sau le poți completa;

f) Dreptul la ștergerea datelor („dreptul de a fi uitat") – poți obține ștergerea datelor, în cazul în care prelucrarea acestora nu a fost legală sau în alte cazuri prevăzute de lege;
g) Dreptul la restricționarea prelucrării - poți solicita restricționarea prelucrării în cazul în care contești exactitatea datelor, precum și în alte cazuri prevăzute de lege;
h) Dreptul de opoziție – poți să te opui, în special, prelucrărilor de date care se întemeiază pe interesul nostru legitim;
i) Dreptul la portabilitatea datelor - poți primi, în anumite condiții, datele personale pe care ni le-ai furnizat, într-un format care poate fi citit automat sau poți solicita ca respectivele date să fie transmise altui operator;
j) Dreptul de a depune plângere - poți depune plângere față de modalitatea de prelucrare a datelor personale la Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal;
k) Dreptul de retragere a consimțământului – în cazurile în care prelucrarea se întemeiază pe consimțământul tău, ți-l poți retrage oricând. Retragerea consimțământului va avea efecte doar pentru viitor, prelucrarea efectuată anterior retragerii rămânând în continuare valabilă;
l) Drepturi suplimentare aferente deciziilor automate: poți cere și obține intervenția umană cu privire la respectiva prelucrare, îți poți exprima propriul punct de vedere cu privire la aceasta și poți contesta decizia.

Art.12. Procedurile prevăzute la alin.(6) trebuie aduse la cunoștința personalului unității și a personalului nou-încadrat în cadrul instructajului realizat anterior acordării drepturilor de utilizator al sistemului informatic. Înainte de începerea activităților de prelucrare a datelor cu caracter personal, utilizatorul trebuie să

semneze o declarație de confidențialitate pe propria răspundere privind respectarea normelor de protecție a acestor date.

(1) Supravegherea prin mijloace audio și/sau video, fixe sau mobile, în scopuri administrative proprii (asigurarea securității incintelor, supravegherea desfășurării unor activități specifice etc.) a unor spații publice din cadrul sediilor unității, a celor perimetrale sau adiacente propriilor sedii constituie o prelucrare a datelor personale. Această operațiune se efectuează pe baza Procedurii de supraveghere video. În acest caz este obligatorie avertizarea personalului propriu și a publicului cu privire la existența sistemului de supraveghere, la scopul prelucrării datelor cu caracter personal și cu privire la datele de identificare ale operatorului.

(2) Instalarea de mijloace audio și/sau video se realizează astfel încât să nu fie vizualizat interiorul altor imobile sau căile de acces la acestea aflate în zona adiacentă echipamentelor de supraveghere, fiind limitat la maximum spațiul public afectat.

Art. 13. Categoriile de destinatari ai datelor cu caracter personal prelucrate de Scoala Gimnaziala Nr. 2 şi structurile sale sunt:

a) Persoana vizată;
b) Reprezentanți legali ai persoanei vizate;
c) Autorități si instituții abilitate)instituțiilor cu atribuții în domeniul apărării, ordinii publice și siguranței naționale, precum și a altor persoane juridice în condițiile legii)

Art. 14. Comunicarea datelor cu caracter personal

(1) Scoala Gimnaziala Nr. 2, primește și soluționează, cererile persoanelor fizice și juridice care au ca obiect furnizarea unor informații ce intră sub incidența Legii nr.190/2018.

(2) Datele personale gestionate de Scoala Gimnaziala Nr. 2 şi structurile sale se comunică la cererea persoanei vizate sau a împuterniciților acesteia, la solicitarea instituțiilor cu atribuții în domeniul apărării, ordinii publice și siguranței naționale, precum și a altor persoane juridice în condițiile legii.

(3) Solicitările privind comunicarea datelor din sistemele de evidență automate și neautomate gestionate de instituțiilor cu atribuții în domeniul apărării, ordinii publice și siguranței naționale, precum și a altor persoane juridice în condițiile legii, trebuie să îndeplinească următoarele cerințe:

a) să fie adresate în formă scrisă, cu precizarea exactă a categoriilor de date cu caracter personal care necesită a fi prelucrate sau, după caz, a drepturilor pe care solicitantul înțelege să le exercite; în situația solicitărilor persoanei vizate depuse în exercitarea drepturilor prevăzute de lege, cererea trebuie să fie scrisă, datată și semnată;
b) să conțină datele necesare identificării persoanei fizice sau juridice care le solicită, precum și motivarea, scopul și durata prelucrării;
c) să cuprindă mențiuni sau să fie însoțite de documente care să facă dovada existenței temeiului legal justificat al solicitării;

(4) Cererile care nu conțin elementele prevăzute la lit. c) se restituie pentru completare iar cele care nu se încadrează în condițiile prevăzute de lege sau de tratatele la care România este parte se resping, menționându-se motivele pentru care comunicarea datelor cu caracter personal nu este posibilă;

(5) Pot face obiectul comunicării doar datele cu caracter personal colectate direct sau indirect de către Scoala Gimnaziala Nr. 2 şi structurile sale, în scopul/scopurile necesare desfășurării activității proprii. Se interzice comunicarea datelor obținute de la alte instituții sau organisme publice, cu excepția situațiilor expres prevăzute de lege.

(6) In situațiile prevăzute în mod expres de lege, datele cu caracter personal pot fi comunicate din oficiu.

(7) Dezvăluirea către terți și transferul de date se efectuează cu informarea persoanei vizate, cu excepția situațiilor prevăzute expres de lege.

(8) Datele asupra cărora persoanele vizate au exercitat și li s-a recunoscut dreptul de opoziție nu pot face obiectul comunicării;

(9) Înainte de comunicarea datelor, Scoala Gimnaziala Nr. 2, prin utilizatorii desemnați, verifică dacă acestea sunt exacte, complete și actualizate. In cazul în

care se constată că datele nu sunt corecte sau actualizate, acestea nu vor fi comunicate și se vor dispune măsuri pentru actualizarea, rectificarea sau ștergerea acestora, după caz.

(10) Datele primite de la alți operatori, organisme publice ori private, nu trebuie să fie prelucrate pentru alte scopuri decât cele specificate în cererea de comunicare sau, după caz, în nota de transmitere.

(11) În situația transmiterii datelor cu caracter personal către terți se va menționa obligația acestora de a nu le prelucra în alte scopuri decât cel pentru care a fost efectuată comunicarea, cu excepția situației în care există consimțământul persoanei vizate sau după solicitarea și primirea acceptului scris din partea Școlii Gimnazială nr 2.

(12) Documentele care conțin date cu caracter personal, transmise persoanei vizate, vor avea înscrisă în subsolul paginii mențiunea: ***„ Datele dumneavoastră sunt prelucrate de Școala Gimnazială nr 2, în conformitate cu Legea nr. 190/2018, în scopul îndeplinirii atribuțiilor legale de operator (persoană împuternicită/ dpo extern). Datele pot fi dezvăluite unor terți în condițiile legii. Vă puteți exercita dreptul de acces, dreptul la rectificare și dreptul la ștergerea datelor (dreptul de a fi uitat), dreptul la restricționarea prelucrării, dreptul la portabilitatea datelor, dreptul de opoziție, dreptul de a nu fi supus unui proces decizional individual automatizat, inclusiv crearea de profiluri, printr-o cerere scrisă, semnată și datată, trimisă pe adresa societății. De asemenea aveți dreptul de a vă adresa cu o plângere la Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal sau justiției, potrivit legii. ”***

(13) Comunicarea trebuie să cuprindă numai datele solicitate expres și doar dacă a fost determinat dreptul terțului de a prelucra acea categorie de date, indiferent de existența sau nu în evidențele Scolii Gimnaziala Nr. 2 şi structurile sale, a altor categorii de date cu caracter personal referitoare la persoana vizată.

(14) In situația în care solicitarea are ca obiect prelucrarea de date cu caracter personal în scopul instrumentării unei cauze penale sau civile, datele solicitate se comunică doar organului de urmărire penală sau instanței de judecată;

(15) Dacă datele cu caracter personal solicitate fac parte din categoria informațiilor clasificate, comunicarea acestora se face cu respectarea strictă a prevederilor legislației privind protecția informațiilor clasificate.

Art. 15. Reguli de prelucrare

(1) Verificarea în sistemele de evidență manuale, automate și, după caz, în dosarele de personal se efectuează de către personalul anume desemnat în baza fișei de post sau prin dispoziții rezolutive ale conducerii Scoala Gimnaziala Nr. 2.

(2) Cu excepția verificării în sistemele de evidență automate unde sistemul este cel care trebuie să genereze fișierul de acces, consemnarea rezultatului verificărilor se efectuează pe baza unor formulare pentru redactarea răspunsurilor care vor fi înregistrate în Registrul special întocmit.

(3) Circuitul formularelor, documentelor și a dosarelor de personal se realizează prin înregistrarea acestora și predarea pe bază de semnătură în condici sau/și registre, conform procedurilor specifice emise la nivelul operatorului.

Art. 16. Consimțământul persoanei vizate

(1) Nici o prelucrare de date cu caracter personal nu poate fi efectuată fără consimțământul persoanei vizate.

(2) Consimțământul persoanei vizate nu este necesar în următoarele cazuri:

a) prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;
b) prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;
c) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;
d) prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul;

e) prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.

(3) În domeniul prelucrării datelor cu caracter personal, consimțământul persoanei vizate reprezintă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate.

(4) Consimțământul poate fi obținut numai după ce persoana vizată a fost complet și exact informată cu privire la scopul prelucrării datelor cu caracter personal care o privesc (Anexa nr.3-Notă de informare).

(5) Consimțământul trebuie dat în mod expres, într-o formă care să permită dovedirea acestuia de către operator.

Secțiunea II. Solicitarea accesului la datele cu caracter personal

Art. 17. Dreptul de acces la date

(l) Orice cerere scrisă prin care o persoană solicită informații despre datele cu caracter personal care o privesc sau despre datele cu caracter personal ale altei persoane pe care o reprezintă în mod legal, se înregistrează în registrul special destinat și, conform dispoziției rezolutive a conducătorului societății, se transmite departamentelor cu competențe în soluționarea acesteia.

(2) Responsabilul cu protecția datelor cu caracter personal este informat cu privire la orice cerere efectuată de către persoana vizată în temeiul Legii nr.190/2018.

(3) Responsabilul cu protecția datelor cu caracter personal stabilește dacă o solicitare se încadrează în categoria "cereri de acces la date cu caracter personal" și intră sub incidența Legii 190/2018, și monitorizează activitatea de soluționare a acestora.

(4) O cerere, pentru a se încadra în categoria "cereri de acces la date cu caracter personal", efectuată în temeiul Legii nr. 190/2018, trebuie să fie scrisă, datată și semnată; astfel, determinarea naturii juridice a solicitării se face prin raportare la conținutul acesteia, nefiind obligatorie, de exemplu, menționarea în cuprinsul acesteia a Legii nr.190/2018 sau existența titulaturii specifice („cerere pentru exercitarea dreptului de acces") ori indicarea în mod expres a dreptului a cărui exercitare se urmărește; în aceste condiții, o cerere în cuprinsul căreia nu există nicio mențiune cu privire la Legea nr. 190/2018 sau cu privire la exercitarea dreptului de acces va fi încadrată în categoria cererilor de acces dacă persoana vizată solicită, de exemplu, confirmarea și/sau comunicarea categoriilor de date cu caracter personal prelucrate cu privire la persoana sa de către operator sau comunicarea scopurilor prelucrărilor efectuate ori dacă, pentru soluționarea cererii, este necesară consultarea log-urilor etc.

(5) O cerere îndeplinește condițiile prevăzute de Legea nr.190/2018 (scrisă, datată și semnată) dacă, în mod rezonabil, se poate constata îndeplinirea acestora; astfel, o cerere transmisă prin intermediul fax-ului sau prin intermediul poștei electronice (scanată în format .pdf) este de natură să îndeplinească aceste condiții.

(6) Orice persoană vizată are dreptul de a obține de la operator, la cerere și în mod gratuit, confirmarea faptului că datele care o privesc sunt sau nu sunt prelucrate de acesta.

(7) Școala Gimnazială nr.2 este obligată, în situația în care prelucrează date cu caracter personal care privesc solicitantul, să comunice acestuia, împreună cu confirmarea, cel puțin următoarele informații:

a) scopurile prelucrării, categoriile de date avute în vedere și destinatarii sau categoriile de destinatari cărora datele cu caracter personal le-au fost sau urmează să le fie divulgate, în special destinatari din țări terțe sau organizații internaționale;
b) acolo unde este posibil, perioada pentru care se preconizează că vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
c) existența dreptului de a solicita operatorului rectificarea sau ștergerea datelor cu caracter personal ori restricționarea prelucrării

datelor referitoare la persoana vizată sau a dreptului de a se opune prelucrării;

d) dreptul de a depune o plângere la autoritatea națională de supraveghere a prelucrării datelor cu caracter personal;
e) în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, orice informații disponibile privind sursa acestora;
f) existența unui proces decizional automatizat incluzând crearea de profiluri, precum și , cel puțin în cazurile respective, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

(8) În cererea transmisă, solicitantul poate arăta dacă dorește ca informațiile să îi fie comunicate la o anumită adresă sau printr-un serviciu de corespondență care să asigure că predarea i se va face numai personal. Cât privește modalitatea de comunicare prin poștă electronică a informațiilor solicitate, aceasta nu are siguranță deplină, astfel că prin alegerea sa solicitantul își asumă riscurile legate de comunicarea electronică de informații (interceptare, modificare, pierdere, distrugere, întârziere în primirea datelor etc.). În această situație, persoana vizată trebuie să fie informată asupra tuturor riscurilor la care este expusă o asemenea comunicare, pentru a consimți expres și neechivoc în alegerea acestei modalități (subliniem că modelul de cerere de acces, pus la dispoziția persoanelor vizate în mod orientativ, informează persoana vizată în mod clar asupra acestor aspecte).

(9) În cazul în care solicitarea nu îndeplinește condițiile prevăzute de lege, solicitantul este informat cu privire la faptul că dreptul de acces se poate exercita doar prin depunerea unei cereri în formă scrisă, datată și semnată.

(10) Odată cu soluționarea unei cererii se aduce la cunoștința persoanelor vizate că au dreptul de a se adresa Autorității naționale de supraveghere sau justiției pentru apărarea drepturilor garantate de lege.

(11) Școala Gimnazială nr.2 este obligată să comunice informațiile solicitate într-un termen rezonabil dar nu mai târziu de 30 zile de la data primirii cererii.

Secțiunea III. Categorii de incidente și soluționarea acestora

Art. 13. (1) Toți utilizatorii sistemului informatic al Scolii Gimnaziala Nr. 2 și structurile sale au acces la date cu caracter personal strict în exercitarea atribuțiilor de serviciu și nu pot să le prelucreze decât pe baza procedurilor interne.

(2) Responsabilul de sistem informatic este obligat să aplice măsurile tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, întrucât prelucrarea comportă transmisii de date în cadrul unei rețele, precum și împotriva oricărei alte forme de prelucrare ilegală.

(3) Incidentele în legătură cu protecția datelor cu caracter personal pot fi:

a) incidente tehnice (electronice);

b) incidente operaționale (fizice);

c) incidente administrative (procedurale).

(4) Incidentul de securitate în domeniul protecției datelor cu caracter personal, stocate sau transmise, reprezintă orice eveniment, acțiune, inacțiune sau împrejurare de natură să afecteze confidențialitatea, integritatea sau disponibilitatea acestor date.

(5) În principal, constituie incident de securitate:

a) pierderea, sustragerea, înlocuirea, alterarea, dezvăluirea sau distrugerea neautorizată ori accidentală a datelor cu caracter personal;

b) forțarea accesului, accesul neautorizat sau interzicerea accesului autorizat la datele cu caracter personal;

c) modificarea neautorizată și nejustificată a datelor cu caracter personal;

d) copierea neautorizată pe suport de date extern sau executarea de fotocopii ale documentelor care conțin date cu caracter personal fără avizul responsabilului cu protecția datelor cu caracter personal și aprobarea șefului departamentului/compartimentului;

e) nerespectarea regulilor privind depozitarea, manipularea sau distrugerea mediilor de stocare în uz pe care sunt stocate date cu caracter personal;

f) nerespectarea prevederilor, metodologiilor, instrucțiunilor și dispozițiilor privind prelucrarea datelor cu caracter personal;

g) distrugerea mediilor de stocare scoase din uz, fără a respecta prevederile actelor normative care reglementează domeniul protecției datelor cu caracter personal.

h) rețele interne nesecurizate;

i) nerespectarea cerințelor legale privind primirea și distribuirea corespondenței în domeniul datelor cu caracter personal;

j) producerea altor evenimente care afectează confidențialitatea, integritatea și disponibilitatea informațiilor clasificate stocate, procesate sau transmise în SIC.

(6) Fiecare incident este investigat de către o comisie formată din Responsabilul cu protecția datelor cu caracter personal desemnat la nivelul societății, un reprezentant al departamentului control/audit/calitate, administratorul bazei de date și șeful nemijlocit al lucrătorului implicat în incident, fiind luate deîndată măsuri de limitare pe cât posibil a prejudiciilor apărute în urma producerii incidentelor apărute.

(7) Investigația stabilește:

a) dacă au fost respectate procedurile privind prelucrarea datelor cu caracter personal;

b) dacă au fost compromise datele cu caracter personal;

c) dacă există persoane care au avut acces la datele cu caracter personal la care se referă incidentul de securitate și stabilirea identității acestora;

d) măsuri preventive, corective sau dacă este cazul măsuri disciplinare.

(8) În cazul în care se constată că au fost compromise datele cu caracter personal se aplică prevederile legale în vigoare.

Secțiunea IV. Cerințele minime de securitate a prelucrării de date cu caracter personal

Art. 14. Cerințele minime de securitate a prelucrărilor de date cu caracter personal stau la baza adoptării și implementării de către Scoala Gimnaziala Nr. 2 a măsurilor tehnice și organizatorice necesare pentru păstrarea confidențialității și integrității datelor cu caracter personal sunt:

(1) Identificarea și autentificarea utilizatorului

a) Prin utilizator se înțelege personalul Școlii Gimnazială nr.2 și structurile sale cu drept de acces la bazele de date cu caracter personal.

b) Pentru buna desfășurare a activității informatice în cadrul Școlii Gimnazială nr.2 și structurile sale, cât și pentru asigurarea confidențialității datelor, a documentelor prelucrate și stocate pe echipamentele de calcul din dotare, precum și protecția și securitatea rețelei informatice, se impune accesarea aplicațiilor din sistemul informatic prin identificarea și autentificarea utilizatorilor.

c) Identificarea și autentificarea în sistem se realizează prin introducerea unui cod de identificare de la tastatura (user-name) — atribuit de către Administratorul sistemului — însoțită de introducerea unei parole.

d) Utilizatorii autorizați ai sistemului informatic răspund pentru securitatea parolelor și a conturilor personale. Codurile de identificare și parolele sunt unice, personale și netransmisibile. Se interzice folosirea lor în comun, de către mai mulți utilizatori.

e) Parolele sunt importante pentru securitatea sistemelor informatice. Ele constituie prima linie de protecție pentru conturile utilizatorilor. Gradul de securitate asigurat de o parolă crește proporțional cu numărul de caractere al acesteia, precum și cu utilizarea atât a literelor, cifrelor și caracterelor speciale; este obligatoriu ca utilizatorul să-și seteze o parolă de minim 7 caractere alfanumerice (obligatoriu cel puțin 3 categorii de caractere din următoarele: litere mici, litere mari, cifre și caractere speciale (*, &, #, etc.)) care să nu conțină date personale (de ex: numele sau prenumele, data nașterii, prenumele membrilor de familie, etc.) sau părți ale numelor acestora și să nu fie folosite pentru a accesa servicii publice (mail, Messenger sau alte conturi pe Internet), sau alte aplicații de interes profesional. Introducerea acestora nu se afișează în clar, pe ecran. Parola nu poate fi schimbată de către utilizator în primele 24 de ore de la ultima setare, sistemul memorând ultimele 24 de parole pentru a nu putea fi refolosite.

f) Durata de valabilitate a parolei este de 90 de zile; înainte de expirarea parolei cu 14 zile utilizatorul va fi înștiințat cu privire la necesitatea schimbării acesteia.

g) O parolă prost aleasă poate duce la compromiterea securității întregii rețele. Prin urmare, este obligatorie respectarea condiției de creare a unei parole cât mai complexe.

h) Este obligatorie schimbarea periodică a parolei și ori de câte ori există posibilitatea ca aceasta să își fi pierdut caracterul confidențial. Este interzisă folosirea parolelor anterioare. Schimbarea parolelor se face numai de către deținătorul acesteia.

i) Parolele nu trebuie să fie inserate în mesajele de poștă electronică sau în alte forme de comunicare electronică; de asemenea, parolele nu vor fi comunicate telefonic; nu este recomandată divulgarea formatului unei parole (în discuțiile cu alte persoane) sau divulgarea parolei în chestionare sau în formulare de securitate.

j) Parolele nu trebuie partajate cu nimeni din societate și trebuie tratate ca fiind informații confidențiale ale societății.

k) Se va evita folosirea opțiunii "Remember password" ("Reține parola").

l) Se interzice transcrierea / păstrarea parolei, la vedere sau în alt mod decât cel prevăzut mai sus ori diseminarea / transmiterea acestora către alte persoane.

m) Documentele care conțin coduri de identificare și parole de acces vor fi arhivate numai dacă acestea nu se mai află în uz.

n) La părăsirea stației de lucru este obligatorie deconectarea utilizatorului (Log off) sau blocarea calculatorului pe contul de utilizator conectat (tasta Windows+L). Deblocarea stației se va putea face doar de către utilizatorul conectat sau administratorul de sistem în caz de necesitate. Această practică este indicată pentru asigurarea securității informațiilor prelucrate și prevenirea accesului neautorizat la aceste informații.

o) La apariția unei situații de modificare a competențelor sau raporturilor de serviciu, la comunicarea Departamentului Resurse Umane sau, unde este cazul, a șefului de departament/compartiment, administratorul de sistem ia măsuri de revocare/suspendare a conturilor de acces, astfel încât prelucrarea datelor cu caracter personal să se facă numai de către personalul autorizat și numai în exercitarea atribuțiilor de serviciu ale acestora.

p) Acordarea de permisiuni suplimentare, restrângerea permisiunilor sau dezactivarea conturilor se face în baza solicitărilor scrise din partea șefilor de departamente/compartimente, în care aceștia vor menționa și motivul acordării,

restrângerii permisiunilor sau dezactivării contului utilizatorului respectiv. Personalul de specialitate al departamentului/compartimentului IT al Școlii Gimnazială nr.2, va răspunde în scris de realizarea cerințelor.

q) La crearea contului de utilizator, specialistul IT setează o parolă temporară, care va fi comunicată în scris — în mod corespunzător titularului de cont, utilizatorul fiind obligat de către sistem să și-o schimbe la prima logare (conectare).

r) Conturile de utilizator care nu au fost folosite mai mult de 90 de zile vor fi dezactivate.

(2) Tipul de acces

a) Tipurile de acces și operațiunile permise acestuia, strict necesare pentru îndeplinirea atribuțiilor de serviciu, se stabilesc conform atribuțiilor din fișa postului fiecărui utilizator.

b) Se interzice accesul dezvoltatorilor de aplicații software/personalului de întreținere a sistemelor informatice la orice fel de date cu caracter personal; în aceste situații, se pun la dispoziția programatorilor/personalului de întreținere numai date anonime.

(3) Păstrarea și utilizarea programelor de sistem și aplicație

a) Instalarea oricărui produs software este interzisă a fi efectuată de către personal neautorizat.

b) Orice instalare sau dezinstalare de produse software se realizează numai de către administratorul de sistem.

c) Este interzisă instalarea oricărui produs software care ar putea periclita securitatea rețelei, cât și introducerea - de către utilizatori - a unor programe răuvoitoare în rețea (viruși, viermi, cai troieni, bombe e-mail).

d) Nicio stație care prelucrează date cu caracter personal nu va fi conectată la INTERNET.

(4) Atribuții și Responsabilități

a) Responsabilii de securitate/sistem:

1. elaborează și propun modificări ale politicii de securitate;

2. elaborează și propun pentru aprobare regulamentele, normele și procedurile de securitate;

3. elaborează proceduri pentru identificarea și monitorizarea activității utilizatorilor;

4. tratează incidentele de securitate în scopul minimizării efectului distructiv al acestora asupra sistemului informatic, cât și a minimizării efectelor negative sau a incorectei funcționări a echipamentelor;

5. instruiesc și evaluează periodic utilizatorii în ceea ce privește cunoașterea și respectarea prevederilor Politicii de securitate, a normelor, regulamentelor sau procedurilor de securitate, prin aplicarea conformă a acestora;

b) Atribuții ale utilizatorilor:

1. să cunoască și să respecte prevederile tuturor regulilor, măsurilor și/sau procedurilor privind securitatea sistemului informatic;

2. să răspundă direct de securitatea și conținutul informațiilor și resursele informatice și de comunicații încredințate;

3. să se asigure că informațiile în posesia cărora intră, sunt transmise numai persoanelor autorizate;

4. le este interzisă mutarea tehnicii de calcul, repoziționarea cablurilor de rețea sau de alimentare, instalarea sau dezinstalarea echipamentelor periferice; aceste operațiuni se realizează prin solicitare scrisă și numai de către administratorul de sistem;

5. să întrețină corespunzător tehnica de calcul din componența sistemului informatic (menținerea curățeniei suprafețelor exterioare, evitarea șocurilor mecanice, etc.);

6. să nu introducă echipamente de calcul sau memorii externe personale (care nu fac parte din sistemul informatic al Școlii Gimnazială nr.2 şi structurile sale); este interzisă scoaterea din cadrul unității a acestor echipamente de calcul sau memorii externe;

7. să informeze persoana vizată atunci când datele cu caracter personal sunt colectate direct de la aceasta, în condițiile legii, cu privire la: identitatea și datele de contact ale operatorului și, după caz, ale reprezentantului acestuia; datele de contact ale responsabilului cu protecția datelor, după caz; scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării; în

cazul în care prelucrarea se face în temeiul articolului 6 alin. (2) lit. (f), interesele legitime urmărite de operator sau de o parte terță; destinatarii sau categoriile de destinatari ai datelor cu caracter personal; dacă este cazul, intenția operatorului de a transfera date cu caracter personal către o țară terță sau o organizație internațională și existența sau absența unei decizii a Comisiei privind caracterul adecvat sau, în cazul transferurilor menționate la art.46 sau 47 sau la art.49 alin. (1) al doilea paragraf, o trimitere la garanțiile adecvate sau corespunzătoare și la mijloacele de a obține o copie a acestora, în cazul în care acestea au fost puse la dispoziție;

8. să prelucreze numai datele cu caracter personal necesare îndeplinirii atribuțiilor de serviciu și să acorde sprijin responsabilului cu protecția datelor cu caracter personal pentru realizarea activităților specifice ale acestuia/acesteia;

9. să păstreze confidențialitatea datelor prelucrate, a contului de utilizator, a parolei/codului de acces la sistemele informatice/baze de date prin care sunt gestionate date cu caracter personal;

10. să respecte măsurile de securitate, precum și celelalte reguli stabilite prin proceduri proprii;

11. să informeze de îndată conducerea Școlii Gimnazială nr.2 şi structurile sale, despre împrejurări de natură a conduce la o diseminare neautorizată de date cu caracter personal sau despre o situație în care au fost accesate/prelucrate date cu caracter personal prin încălcarea normelor legale, despre care a luat la cunoștință;

12. la sfârșitul programului este obligatorie închiderea calculatoarelor și a imprimantelor, precum și a celorlalte echipamente periferice, dacă este cazul.

(5) Folosirea computerelor, aplicațiilor informatice

a) Utilizarea aplicațiilor informatice se face numai în conformitate cu procedurile, normele de lucru și metodologiile de exploatare aprobate.

b) Accesarea informațiilor stocate în bazele de date se realizează numai în interesul îndeplinirii atribuțiilor profesionale, iar furnizarea acestor informații este permisă numai în conformitate cu prevederile legale.

c) Utilizatorii trebuie să anunțe responsabilul de sistem când observă:

1. posibilă problemă / breșă în sistemul de securitate al sistemului informatic;

2. o posibilă întrebuinţare greşită sau încălcare a regulamentelor în vigoare;

3. o funcţionare anormală a echipamentelor de calcul.

d) Utilizatorii, prin acţiunile lor, nu trebuie să încerce să compromită protecţia sistemelor informatice şi de comunicaţii şi nu trebuie să desfăşoare, deliberat sau accidental, acţiuni care pot afecta confidenţialitatea, integritatea şi disponibilitatea informaţiilor de orice tip în cadrul sistemului informatic.

e) Utilizatorii nu trebuie să încerce să obţină acces la date sau programe din SIC-urile pentru care nu au autorizaţie.

f) Utilizatorilor autorizaţi li se interzice să permită altor persoane, inclusiv altor utilizatori autorizaţi, accesarea sistemului informatic cu contul şi parola lor sau cu alte elemente de identificare personală.

g) Conturile şi parolele asociate sunt personale. Utilizatorii au obligaţia de a schimba parola propriului cont ori de câte ori există suspiciunea că aceasta este cunoscută şi de alte persoane.

h) Utilizatorii nu trebuie să facă copii neautorizate sau să distribuie materiale protejate prin legile privind proprietatea intelectuală (copyright).

i) Accesul în încăperile în care se află echipamente care prelucrează date cu caracter personal este strict limitat la utilizatorii cu atribuţii în acest domeniu.

j) Accesul pentru intervenţii tehnice, reparaţii sau activităţi de deservire la echipamentele informatice, este permis numai angajaţilor care deţin autorizaţii de acces, fiind însoţiţi permanent de către un lucrător anume desemnat de către şeful departamentului/compartimentului.

k) Accesul angajaţilor altor societăţi care efectuează lucrări de construcţii, reparaţii şi întreţinere a clădirii, instalaţiilor sau utilităţilor în zonele administrative ori în zonele de securitate se realizează cu documente de acces temporar eliberate de şeful departamentului/compartimentului administrativ, pe baza actelor de identitate, la solicitarea reprezentanţilor autorizaţi ai societăţilor în cauză.

l) Accesul persoanelor din afara societăţii în zona administrativă sau în zonele de securitate este permis numai însoţite de persoane anume desemnate, cu permis de acces eliberat la punctul de control-acces, pe baza documentelor de legitimare, după ce au fost înregistrate în registrul de acces în societate.

m) Este interzis accesul în sediul societății cu aparate de fotografiat, filmat, înregistrat audio-video, de copiat din baze de date informatice sau de comunicare la distanță.

n) Sistemul de control-acces asigură prevenirea pătrunderii neautorizate în sediul serviciului, sectoarele și locurile unde sunt gestionate informații clasificate.

o) Accesul la stațiile de lucru este permis numai personalului autorizat, și numai în baza datelor de acces (cont de utilizator si parolă).

p) Produsul software antivirus este instalat pe toate serverele și stațiile și se actualizează automat zilnic; acesta este administrat și monitorizat de către personalul de specialitate al Școlii Gimnazială nr.2

(6) Instruirea personalului

a) Instruirea personalului cu privire la protecția și prelucrarea datelor cu caracter personal și libera circulație a acestor date se efectuează în cadrul programului de pregătire continuă sau ori de câte ori este nevoie, conform dispozițiilor primite.

(7) Imprimarea datelor

a) Tipărirea la imprimantă a datelor cu caracter personal se va realiza numai de utilizatori autorizați pentru această operațiune.

b) Utilizatorii sunt obligați sa respecte procedurile interne specifice, precum și Politica de securitate în sistemul informatic.

Titlul V. DISPOZIŢII FINALE

Art. 15. Documentul se difuzează întregului personal al Scolii Gimnaziala Nr. 2 şi structurile sale

Art. 16. Procedura va fi revizuite în cazul în care apar modificări organizatorice sau ale reglementărilor legale cu caracter general și intern pe baza cărora se desfășoară activitățile care fac obiectul acestor proceduri.

Art. 17. Pe perioada absenței de la serviciu a persoanelor care utilizează procedura în forma inițială sau revizuită, aplicarea acestora se va realiza și de înlocuitorii acestor persoane.

Art. 18. Anexele 5 și 6 se păstrează la emitent.

Art. 19. Prezenta procedură intră în vigoare la data avizării de către Responsabilului cu Protecția Datelor Personale și aprobării de către conducerea Școlii Gimnazială nr.1

Art. 20. Anexele 1 – 6 fac parte integrantă din prezenta politică.

Anexa nr.1 -Declarație (confidențialitate)

Anexa nr.2 -Acordul personalului angajat

Anexa nr. 3 - Nota de informare persoane vizate

Anexa nr. 4 – Registru de evidenta(cartografiere)

Anexa nr. 5 Lista de difuzare a procedurilor

Anexa nr. 6 - Lista reviziilor