PROCEDURĂ OPERAȚIONALĂ

MONITORIZAREA AUDIO-VIDEO ÎN SĂLILE DE CLASĂ ȘI ÎN SPAȚIUL ȘCOLAR

Ediția I, Revizia 0

Data: 10.09.2026

Colegiul Național „Iancu de Hunedoara”

Hunedoara

1. Lista responsabililor cu elaborarea, verificarea și aprobarea ediției sau, după caz, a reviziei în cadrul ediției procedurii

Nr. crt.	Elemente privind responsabilii/operațiunea	Numele și prenumele	Funcția	Data	Semnătura
0	1	2	3	4	5
1.	Elaborat	Lucian Maier	Director adjunct	10.09.2026	[redacted]
2.	Verificat	Olguța Băncușel	Director adjunct	10.09.2026	
3.	Avizat	Cristina Mariș	Coordonator CEAC	10.09.2026	
4.	Aprobat	Maria Cristea	Director	10.09.2026	

2. Situația edițiilor și a reviziilor în cadrul edițiilor procedurii

Nr. crt.	Ediția sau revizia	Componentă revizuită	Modalitatea reviziei	Data aplicării
0	1	2	3	4
	Ediția I	Document inițial	Elaborarea procedurii în aplicarea art. 66 din Legea nr. 198/2023 și a O.M.E.C. nr. 3781/2025.	10.09.2026

3. Lista cuprinzând persoanele la care se difuzează ediția sau, după caz, revizia din cadrul ediției procedurii

Nr. crt.	Scopul difuzării	Exemplar nr.	Compartiment / categorie	Funcția	Numele și prenumele	Semnătura
0	1	2	3	4	5	6
	Aplicare		Conducere; personal desemnat pentru sistem; responsabil protecția datelor	Conform deciziilor interne		
	Informare		Personal didactic, didactic auxiliar și administrativ; elevi; părinți/reprezentanți legali	—		
	Evidență		CEAC / responsabil proceduri	Coordonator CEAC	Cristina Mariș	
	Arhivare		Arhivă	Arhivar		

4. Scopul procedurii

Prezenta procedură stabilește cadrul intern pentru instalarea, punerea în funcțiune, utilizarea, administrarea, stocarea, accesarea și ștergerea înregistrărilor realizate prin sistemele de monitorizare audio-video din Colegiul Național „Iancu de Hunedoara”, cu accent pe monitorizarea în sălile de clasă.

Procedura urmărește simultan două obiective care trebuie respectate împreună: creșterea siguranței elevilor și a personalului și protejarea vieții private, a demnității și a libertății profesionale a persoanelor aflate în spațiul școlar.

Sistemul nu este un instrument de supraveghere pedagogică sau managerială a lecțiilor. Înregistrările nu se utilizează pentru evaluarea profesională a cadrelor didactice, pentru observarea curentă a modului de predare, pentru verificarea metodelor didactice, a ritmului lecției ori a relației pedagogice în afara unei situații care intră în scopurile legale ale monitorizării și nu se utilizează pentru soluționarea contestațiilor privind evaluarea elevilor.

În raport cu elevii, sistemul are rol de protecție și de clarificare a unor incidente relevante pentru siguranță, violență ori protecția bunurilor; nu este destinat urmăririi permanente a comportamentului obișnuit din clasă și nici transformării fiecărei abateri minore într-o verificare video.

5. Domeniul de aplicare

Procedura se aplică sistemelor audio-video utilizate în spațiile Colegiului în care legea permite monitorizarea: săli de clasă, exteriorul clădirilor, holuri, săli de festivități, holurile căminelor/internatelor, dacă este cazul, precum și săli de sport. Este interzisă instalarea camerelor în vestiare și grupuri sanitare.

Procedura se aplică tuturor persoanelor vizate de monitorizare - elevi minori și majori, personal, părinți/reprezentanți legali și alte persoane care intră în zonele monitorizate - precum și persoanelor cărora li se acordă atribuții tehnice, administrative sau de acces.

Supravegherea audio-video realizată în cadrul examenelor și concursurilor naționale este supusă reglementărilor speciale aplicabile acelor examene/concursuri. Dacă este folosită aceeași infrastructură tehnică, regulile privind examenul prevalează pentru înregistrările realizate în acel context.

Documente de referință aplicabile activității procedurale

- Legea învățământului preuniversitar nr. 198/2023, cu modificările și completările ulterioare, în special art. 66;
- Ordinul ministrului educației și cercetării nr. 3781/15.04.2025 pentru aprobarea Procedurii privind monitorizarea audio-video în cadrul unităților de învățământ preuniversitar;
- Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal (GDPR);
- Legea nr. 190/2018 privind măsuri de punere în aplicare a GDPR, cu modificările ulterioare;
- Legea nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor, cu modificările și completările ulterioare, și H.G. nr. 301/2012;
- Ordinul ministrului educației nr. 6235/2023 privind procedura de management al cazurilor de violență, cu modificările ulterioare;
- Regulamentul-cadru de organizare și funcționare a unităților de învățământ preuniversitar, aprobat prin O.M.E. nr. 5726/2024, cu modificările și completările ulterioare;
- Regulamentul de organizare și funcționare al Colegiului Național „Iancu de Hunedoara”, în vigoare;
- Ghidul nr. 3/2019 al Comitetului European pentru Protecția Datelor privind prelucrarea datelor cu caracter personal prin mijloace video;
- Ordinul S.G.G. nr. 600/2018 privind aprobarea Codului controlului intern managerial al entităților publice și Instrucțiunea nr. 1/2018 privind Standardul 9 - Proceduri.

6. Definiții și abrevieri ale termenilor utilizați

Nr. crt.	Termenul	Definiția
1	Operator de date	Colegiul Național „Iancu de Hunedoara”, care stabilește scopurile și mijloacele prelucrării datelor prin sistemul audio-video.
2	Persoană vizată	Persoana fizică identificată sau identificabilă surprinsă de sistemul audio-video: elev, salariat, părinte, vizitator sau altă persoană.
3	Sistem de monitorizare audio-video	Ansamblul camerelor, microfoanelor dacă sunt activate, echipamentelor de înregistrare, serverelor/NVR/DVR, monitoarelor, cablurilor, aplicațiilor și mecanismelor de acces și

		stocare.
4	Înregistrare	Fișierul ori secvența de date audio-video creată de sistem.
5	Flux în timp real (live)	Imaginea și, dacă este activată legal, componenta audio disponibilă în momentul captării, înainte de consultarea arhivei.
6	Vizualizare	Acces autorizat la o înregistrare, realizat fără furnizarea unei copii persoanei solicitante, în condițiile legii.
7	Conservare	Măsura tehnică prin care o secvență relevantă este protejată de ștergerea automată la împlinirea termenului de 30 de zile, atunci când există o cercetare/sesizare temeinic justificată.
8	Extragere	Copierea controlată a unei secvențe pe un suport securizat, exclusiv atunci când este necesară pentru conservare, pentru o procedură legală sau pentru punerea la dispoziția organelor competente.
9	Incident de securitate	Orice acces neautorizat, divulgare, pierdere, alterare, distrugere, copiere nepermisă ori indisponibilitate relevantă a datelor sau sistemului.
10	EIPD / DPIA	Evaluarea impactului asupra protecției datelor, efectuată înainte de punerea în funcțiune și revizuită atunci când se schimbă semnificativ riscul ori configurația prelucrării.

Abrevieri

Nr. crt.	Abrevierea	Termenul abreviat
1	CA	Consiliul de administrație
2	PO	Procedură operațională
3	DPO/RPD	Responsabil cu protecția datelor
4	EIPD	Evaluarea impactului asupra protecției datelor
5	NVR/DVR	Echipament de înregistrare în rețea/digitală

7. Descrierea procedurii

7.1. Principii de bază

- legalitate, necesitate și proporționalitate: monitorizarea se realizează numai în spațiile și în condițiile permise de lege și numai atât timp cât este justificată;
- scop determinat: înregistrările sunt folosite numai pentru prevenirea și cercetarea cazurilor de violență fizică sau psihică și pentru protecția persoanelor, bunurilor și valorilor, în limitele legii;
- minimizarea datelor: se evită captarea unor zone, intervale, sunete ori informații care nu sunt necesare scopului urmărit;
- confidențialitate: imaginile și sunetul, dacă există, nu sunt materiale publice și nu circulă în grupuri, pe telefoane personale, platforme de mesagerie sau rețele sociale;
- acces controlat și trasabil: orice acces la arhivă este justificat, autorizat și consemnat;
- protecția mediului educațional: existența camerelor nu transformă ora de curs într-o inspecție permanentă și nu afectează autonomia profesională legitimă a cadrului didactic;
- protecția elevului: monitorizarea este utilizată pentru siguranță și clarificarea unor situații relevante, fără stigmatizare, expunere publică sau revictimizare.

7.2. Interdicții exprese privind utilizarea sistemului

Pentru a proteja în mod real încrederea personalului și a elevilor, următoarele utilizări sunt interzise:

- vizualizarea în timp real a unei ore de curs de către conducere în scop de control managerial, pedagogic sau de evaluare a cadrului didactic;
- consultarea aleatorie sau periodică a arhivei pentru a observa „cum se desfășoară orele”, fără existența unei situații concrete care intră în scopurile legale ale sistemului;
- folosirea înregistrărilor pentru evaluarea profesională, inspecția la clasă, acordarea calificativului, aprecierea metodelor de predare, ritmului lecției, stilului pedagogic ori a relației profesor-elev, în afara cercetării unei situații de violență/siguranță permise de lege;
- folosirea înregistrărilor pentru soluționarea contestațiilor privind notele sau evaluarea elevilor la orele de curs;
- folosirea sistemului ca mecanism obișnuit de verificare a întârzierilor, temelor, uniformei, telefonului mobil, vorbitului în timpul orei ori a altor abateri minore care nu țin de violență sau protecția persoanelor/bunurilor;
- furnizarea de copii către părinți, elevi sau salariați atunci când legea prevede accesul numai prin vizualizare;
- fotografierea sau filmarea monitorului cu telefonul ori alt dispozitiv personal în timpul unei vizualizări;
- publicarea, transmiterea pe rețele sociale, grupuri de mesagerie sau către presă a înregistrărilor.

7.3. Etapa prealabilă instalării/punerii în funcțiune

1. Conducerea întocmește o analiză de necesitate care indică spațiile vizate, riscurile care justifică monitorizarea, programul de funcționare și măsurile mai puțin intruzive deja existente sau analizate.
2. Se realizează inventarierea tehnică a sistemului: tipul camerelor, existența funcției audio, unghiurile de captare, NVR/DVR/server, capacitatea efectivă de stocare, controlul accesului, posibilitatea ștergerii automate și existența jurnalelor tehnice.
3. Înainte de activarea monitorizării curente în sălile de clasă, sistemul trebuie configurat astfel încât să poată asigura termenul legal de stocare de 30 de zile, precum și ștergerea automată la expirarea acestuia, cu excepția secvențelor conservate în cazurile justificate.
4. Se efectuează EIPD, cu implicarea responsabilului cu protecția datelor. Evaluarea cuprinde necesitatea și proporționalitatea prelucrării, riscurile pentru elevi și personal, măsurile tehnice și organizatorice, accesul, stocarea, funcția audio, informarea și modul de exercitare a drepturilor.
5. Dacă echipamentele permit captarea sunetului, activarea funcției audio nu se consideră automată. Necesitatea ei se analizează distinct în EIPD, în raport cu principiul minimizării datelor. Dacă scopul poate fi atins în mod rezonabil numai prin imagine, funcția audio se menține dezactivată.

7.4. Consultarea, acordul și hotărârea Consiliului de administrație

În situația obișnuită, instalarea și/sau punerea în funcțiune a sistemului se realizează după procedura de consultare prevăzută de lege și de O.M.E.C. nr. 3781/2025. Se întocmește lista salariaților, a părinților/reprezentanților legali ai elevilor minori și a elevilor majori, iar exprimarea sau neexprimarea acordului se centralizează într-un proces-verbal.

Decizia se poate lua atunci când există acordul majorității simple a persoanelor din categoriile prevăzute de lege care au participat la luarea deciziei, în condițiile actului normativ aplicabil. Pentru un elev minor, acordul sau lipsa acordului se exprimă de un singur părinte/reprezentant legal.

În situații excepționale, atunci când există un risc crescut de violență în spațiul școlar, un număr semnificativ de sesizări privind acte de violență fizică și/sau psihică ori săvârșirea unei fapte prevăzute de legea penală, se aplică regimul special prevăzut de lege, care poate permite luarea deciziei prin informarea persoanelor vizate, cu respectarea celorlalte condiții legale.

Hotărârea de instalare și/sau punere în funcțiune se adoptă de CA pentru o perioadă de maximum un an calendaristic. Prelungirea se face numai printr-o nouă hotărâre, dacă circumstanțele se mențin și după parcurgerea cerințelor legale aplicabile. Consultarea personalului și informarea persoanelor vizate se consemnează.

7.5. Informarea persoanelor vizate și semnalizarea

- înainte de punerea în funcțiune, se publică pe site și se afișează la avizier nota de informare privind prelucrarea datelor;
- la intrările în zonele monitorizate și în locuri ușor vizibile se amplasează pictograma/semnul de monitorizare audio-video;
- informarea explică pe înțelesul elevilor și al personalului scopul sistemului, cine este operatorul, termenul de 30 de zile, cine poate avea acces, cum se formulează o cerere și cui se adresează întrebările privind datele personale;
- informarea nu prezintă camerele ca instrument de control al profesorilor sau al elevilor și precizează expres interdicțiile privind evaluarea profesională și contestațiile la evaluarea elevilor.

7.6. Amplasarea și funcționarea camerelor

Camerele se amplasează numai în spațiile permise de lege. Unghiurile se configurează astfel încât să acopere zona necesară și să evite, pe cât posibil, captarea excesivă a unor spații care nu servesc scopului monitorizării.

În sălile de clasă, sistemul funcționează potrivit hotărârii CA și configurației aprobate. Cadrele didactice și elevii nu au obligația de a acționa camera, de a o porni/opri sau de a gestiona suportul de stocare, cu excepția persoanelor desemnate prin decizie.

Nu se instalează și nu se utilizează camere ascunse. Monitoarele care afișează imagini sunt poziționate în spații cu acces controlat, astfel încât imaginile să nu fie vizibile publicului sau persoanelor neautorizate.

Sistemul este configurat cu circuit închis și fără posibilitatea de configurare sau acces din afara unității. Nu se utilizează conturi personale, stocare personală în cloud, aplicații de mesagerie sau dispozitive private pentru accesarea arhivei.

7.7. Vizualizarea în timp real

Vizualizarea în timp real a sălilor de clasă nu se realizează ca activitate obișnuită de conducere, control sau observație pedagogică. Fluxul live poate fi accesat de persoane autorizate numai atunci când există o nevoie concretă de siguranță sau protecție imediată, pentru gestionarea unui incident în desfășurare ori pentru verificări tehnice strict necesare.

O verificare tehnică se limitează la durata și imaginile necesare pentru a confirma funcționarea echipamentului; nu se transformă într-o observare a lecției.

7.8. Stocarea și ștergerea înregistrărilor

Înregistrările se păstrează în condiții de siguranță și confidențialitate timp de 30 de zile, după care se șterg automat. Sistemul trebuie verificat periodic pentru a se confirma că mecanismul de ștergere automată funcționează.

În cazuri temeinic justificate, atunci când o secvență este relevantă pentru cercetarea unei sesizări sau a unui incident permis de lege, aceasta poate fi conservată peste termenul de 30 de zile până la finalizarea cercetărilor. Conservarea se dispune în scris, se consemnează în registru, se limitează la intervalul necesar și se păstrează separat/securizat.

La încetarea motivului de conservare, înregistrarea se șterge fără întârziere, dacă nu există o obligație legală distinctă de păstrare sau o solicitare a organelor competente.

7.9. Accesul la înregistrări

Accesul persoanelor îndreptățite se face numai în baza unei cereri scrise și motivate, aprobate de director, și numai prin vizualizare, în condițiile legii. Cererea trebuie să indice suficient de precis motivul, data și intervalul de timp solicitat. Formulări generale de tipul „doresc să văd ce se întâmplă la clasă” nu justifică accesul.

Pot solicita acces, în condițiile legii, părintele/reprezentantul legal al elevului minor, elevul major, personalul unității, reprezentanții autorităților prevăzute de lege și consilierul/psihologul școlar în condițiile speciale aplicabile acestuia.

Vizualizarea se realizează într-un spațiu controlat, pe echipamentul unității, în prezența persoanei autorizate să gestioneze accesul. Solicitantului nu i se permite conectarea unui dispozitiv personal, copierea fișierului, fotografierea sau filmarea ecranului.

Atunci când în secvență apar persoane terțe fără legătură cu situația cercetată, se aplică, în măsura posibilităților tehnice, mascarea/distorsionarea acestora ori se limitează intervalul vizualizat. Dacă mascarea nu este tehnic posibilă, vizualizarea se organizează astfel încât ingerința în drepturile terților să fie minimă.

Fiecare acces este înregistrat în Registrul de acces: data, persoana, temeiul, numărul cererii, intervalul vizualizat, persoanele prezente, eventualele operațiuni tehnice efectuate și semnăturile.

7.10. Cercetarea incidentelor de violență și protecția elevului

Înregistrarea poate constitui un element de clarificare a unui incident, dar nu înlocuiește procedurile legale de management al violenței, audierea/ascultarea persoanelor în condițiile legii, evaluarea contextului și măsurile de protecție.

În cazurile care implică minori, accesul și utilizarea secvențelor se realizează cu evitarea revictimizării, expunerii inutile și confruntării publice. Secvențele nu se proiectează în fața clasei și nu se utilizează pentru umilirea ori stigmatizarea unei persoane.

Dacă o înregistrare indică o posibilă faptă penală sau este solicitată de organele de urmărire penală, unitatea asigură conservarea și punerea la dispoziție în condițiile solicitării legale, cu consemnarea operațiunii.

7.11. Extragerea și transmiterea înregistrărilor

Extragerea unei copii nu se face pentru uzul obișnuit al părinților, elevilor sau salariaților. Ea este permisă numai pentru conservare internă justificată ori pentru transmiterea către organele/autoritățile competente atunci când există un temei legal sau o solicitare oficială.

Fișierul extras se denumește neutru, se păstrează pe suport securizat, se protejează împotriva modificării și accesului neautorizat, iar predarea se realizează pe bază de proces-verbal, cu identificarea fișierului, intervalului, suportului, persoanei care a extras și destinatarului.

Orice copie de lucru rămasă în sistemul unității după predare este eliminată când nu mai este necesară, cu respectarea obligațiilor legale.

7.12. Măsuri tehnice și organizatorice de securitate

- spațiul în care se află NVR/DVR/serverul este încuiat și accesibil numai persoanelor desemnate;
- conturile de acces sunt individuale; conturile comune se evită, iar parolele sunt suficient de complexe, schimbate la nevoie și revocate imediat la schimbarea atribuțiilor;
- se activează, dacă sistemul permite, jurnalizarea accesărilor și a operațiunilor efectuate; dacă nu permite, se ține registrul administrativ de acces;
- monitoarele nu sunt orientate către zone accesibile publicului și nu rămân nesupravegheate cu imagini afișate;
- operațiunile de mentenanță se fac, de regulă, la sediul unității, fără acces de la distanță la înregistrări; furnizorii sunt informați asupra obligațiilor de confidențialitate și au acces numai dacă este strict necesar și controlat;
- nu se folosesc stick-uri USB personale; suporturile autorizate sunt inventariate, păstrate securizat și șterse controlat;

- se fac verificări periodice privind data/ora sistemului, capacitatea de stocare de 30 de zile, ștergerea automată, camerele nefuncționale, jurnalizarea și tentativa de acces neautorizat;
- orice incident de securitate se raportează imediat directorului și responsabilului cu protecția datelor.

7.13. Incidente de securitate și încălcări ale datelor

Persoana care constată pierderea unui fișier, accesul neautorizat, copierea sau publicarea unei înregistrări, compromiterea unei parole, defectarea severă a sistemului ori alt incident de securitate informează imediat directorul și responsabilul cu protecția datelor și nu încearcă să ascundă sau să remedieze informal situația.

Se iau măsuri pentru limitarea incidentului, conservarea jurnalelor și stabilirea persoanelor/înregistrărilor afectate. Responsabilul cu protecția datelor sprijină evaluarea obligației de notificare a autorității de supraveghere și, dacă este cazul, a persoanelor vizate, în termenele prevăzute de GDPR.

Incidentul și măsurile corective se documentează. Parolele și drepturile de acces se schimbă/retrag imediat atunci când există suspiciunea compromiterii lor.

7.14. Drepturile persoanelor vizate

Persoanele vizate primesc informațiile prevăzute de GDPR și pot formula cereri privind drepturile lor, în limitele în care acestea sunt aplicabile prelucrării audio-video și fără a afecta drepturile și libertățile altor persoane ori obligațiile legale ale unității.

Cererea privind accesul la înregistrări în sensul prezentei proceduri se soluționează potrivit regimului special prevăzut de Legea nr. 198/2023 și O.M.E.C. nr. 3781/2025. Cererile generale privind protecția datelor sunt transmise responsabilului cu protecția datelor.

7.15. Revizuirea periodică a necesității monitorizării

Existența tehnică a camerelor nu înseamnă că monitorizarea trebuie menținută nelimitat. Cel puțin la expirarea perioadei aprobate de CA și ori de câte ori se schimbă semnificativ riscurile, amplasarea sau configurația, conducerea reanalizează necesitatea și proporționalitatea măsurii.

Prelungirea monitorizării în clase se motivează prin situația concretă a unității și nu se face automat. EIPD și nota de informare se actualizează atunci când modificările de sistem ori de scop impun acest lucru.

8. Responsabilități

Consiliul de administrație

- analizează necesitatea și proporționalitatea monitorizării și hotărăște instalarea/punerea în funcțiune pentru perioada legală;
- stabilește persoana care răspunde de gestionarea și funcționarea sistemului și aprobă, la nivel instituțional, amplasarea camerelor și măsurile de securitate;
- verifică la prelungire dacă se mențin circumstanțele care au justificat măsura.

Directorul

- emite deciziile interne necesare aplicării hotărârii CA și desemnează persoanele autorizate;
- aprobă sau respinge motivat cererile de vizualizare, în limitele legii;
- dispune, când este justificat, conservarea secvențelor relevante și punerea la dispoziția organelor competente;
- asigură că sistemul nu este folosit pentru evaluarea profesională a cadrelor didactice ori pentru contestații la evaluarea elevilor;
- dispune măsuri la incidente de securitate și la accesări neautorizate.

Responsabilul cu gestionarea și funcționarea sistemului audio-video

- verifică funcționarea camerelor, data/ora, capacitatea de stocare, ștergerea automată și jurnalele;
- administrează accesul tehnic în limitele drepturilor acordate și nu vizualizează înregistrări din curiozitate sau fără temei;
- realizează, la dispoziția autorizată, conservarea/extragerea secvențelor și completează registrele;
- raportează imediat defecțiunile și incidentele.

Responsabilul cu protecția datelor (DPO/RPD)

- consiliază unitatea cu privire la legalitatea, necesitatea și proporționalitatea monitorizării;
- coordonează/avizează EIPD și actualizarea acesteia;
- verifică informările, măsurile de securitate, accesul și respectarea termenelor de stocare;
- sprijină soluționarea cererilor persoanelor vizate și gestionarea incidentelor de date.

Comisia pentru prevenirea și combaterea violenței / personalul care gestionează un caz

- solicită acces numai pentru o situație concretă care intră în scopurile legale ale sistemului;
- utilizează înregistrarea ca element de clarificare, împreună cu celelalte informații și proceduri aplicabile;
- protejează identitatea și demnitatea elevilor și evită revictimizarea ori difuzarea inutilă a secvențelor.

Secretariatul

- înregistrează cererile de vizualizare și documentele oficiale privind solicitarea/predarea înregistrărilor;
- asigură circuitul documentelor către director și, după caz, către responsabilul desemnat, fără a accesa conținutul video.

Personalul didactic, didactic auxiliar și administrativ

- respectă caracterul confidențial al sistemului și nu solicită acces decât în condițiile procedurii;
- nu fotografiază, nu filmează și nu distribuie imagini de pe monitoare sau din arhivă;
- raportează defecțiunile, incidentele și orice suspiciune de acces neautorizat.

Furnizorii / personalul tehnic extern

- intervin numai în baza unui raport contractual și a unei solicitări autorizate, cu respectarea confidențialității;
- nu primesc acces permanent la imagini și nu realizează acces de la distanță la arhivă;
- nu copiază și nu păstrează înregistrări ale unității.

CEAC / responsabilul cu procedurile

- ține evidența controlată a procedurii și a reviziilor acesteia;
- semnalează necesitatea actualizării documentului atunci când cadrul normativ sau fluxul intern se modifică.

9. Formulare

Formularele de mai jos fac parte din prezenta procedură și pot fi adaptate grafic fără modificarea conținutului esențial.

F-01 – Proces-verbal de consultare și centralizare a acordurilor

Data: ..... Perioada pentru care se propune monitorizarea: .....

Spațiile vizate: .....

Temeiul și motivarea măsurii: .....

Categoria	Număr persoane pe listă	Au participat	Acord	Dezacord / fără opțiune
Părinți/reprezentanți legali ai elevilor minori				
Elevi majori				
Salariați				

Concluzie privind îndeplinirea condițiilor legale: .....

Semnături persoane responsabile de centralizare: .....

F-02 – Cerere motivată de vizualizare a unei înregistrări audio-video

Subsemnatul/Subsemnata ....., în calitate de .....,

solicit vizualizarea înregistrării aferente datei ....., intervalului orar ..... - ....., spațiul/clasa ..... .

Motivarea concretă a solicitării:
.....
.....

Persoana/elevul la care se referă situația, dacă este cazul: .....

Declar că am luat la cunoștință faptul că accesul se realizează numai în condițiile legii și, de regulă, numai prin vizualizare; nu voi fotografia/filma ecranul și nu voi publica ori utiliza imaginile pentru prejudicierea persoanelor.

Data ..... Semnătura .....

Rezoluția directorului: □ APROBAT □ RESPINS

Motivare/condiții: .....

Data ..... Director .....

F-03 – Registrul accesului la înregistrările audio-video

Nr.	Data/ora	Cerere / temei	Solicitant	Interval vizualizat	Persoane prezente	Operațiuni efectuate	Semnături

F-04 – Proces-verbal de conservare/extragere/punere la dispoziție

Nr. ...../Data .....

Tip operațiune: □ conservare internă □ extragere □ predare către autoritate competentă

Motivul/temeiul: .....

Înregistrarea: data ....., interval ..... - ....., camera/spațiul .....

Identificarea fișierului/suportului și, dacă este disponibilă, valoarea de verificare/hash: .....

Persoana care a efectuat operațiunea: .....

Locul securizat de păstrare / destinatarul: .....

Termenul sau evenimentul la care încetează conservarea: .....

Observații: .....

Semnături: .....

F-05 – Fișă de incident tehnic/de securitate privind sistemul audio-video

Data și ora constatării: ..... Persoana care raportează: .....

Tip incident: □ acces neautorizat □ divulgare/copiere □ parolă compromisă □ pierdere/ștergere □ defectare □ altul

Descriere:
.....
.....

Camere/înregistrări/persoane posibil afectate: .....

Măsuri imediate luate: .....

Director informat la: ..... DPO/RPD informat la: .....

Necesitatea evaluării unei notificări GDPR: □ da □ nu □ în analiză

Măsuri corective și data închiderii incidentului: .....

Semnături: .....

F-06 – Model scurt de informare pentru zonele monitorizate

ZONĂ MONITORIZATĂ AUDIO-VIDEO

Operator: Colegiul Național „Iancu de Hunedoara”. Scop: protecția persoanelor, bunurilor și valorilor și prevenirea/cercetarea faptelor de violență, în condițiile legii. Înregistrările sunt păstrate, de regulă, 30 de zile și nu sunt utilizate pentru evaluarea profesională a cadrelor didactice ori pentru contestații privind evaluarea elevilor. Detalii privind prelucrarea datelor, accesul și drepturile persoanelor vizate sunt disponibile la avizier/site și prin responsabilul cu protecția datelor.

F-07 – Fișă periodică de verificare a funcționării și conformității

Element verificat	Conform	Neconform / observații	Măsură și termen
Data și ora sistemului sunt corecte	□ Da □ Nu		
Toate camerele aprobate funcționează	□ Da □ Nu		
Capacitatea efectivă de stocare asigură 30 de zile	□ Da □ Nu		
Ștergerea automată funcționează	□ Da □ Nu		
Accesul din exteriorul unității este dezactivat	□ Da □ Nu		
Conturile și parolele persoanelor autorizate sunt actuale	□ Da □ Nu		
Monitoarele și serverul sunt protejate fizic	□ Da □ Nu		
Jurnalele de acces / registrul sunt actualizate	□ Da □ Nu		
Semnalizarea și nota de informare sunt afișate	□ Da □ Nu		
Secvențele conservate au temei și termen urmărit	□ Da □ Nu		

Data verificării: ..... Persoana responsabilă: ..... Semnătura: .....

10. Dispoziții finale

Prezenta procedură se aplică împreună cu legislația în vigoare, cu Regulamentul de organizare și funcționare al Colegiului și cu procedura privind managementul cazurilor de violență.

Dacă o prevedere internă intră în contradicție cu o dispoziție legală ulterioară, se aplică norma legală, iar procedura se revizuiește în cel mai scurt timp.

Nicio prevedere a prezentei proceduri nu poate fi interpretată în sensul instituirii unui drept al conducerii, al personalului, al părinților sau al elevilor de a urmări în mod liber activitatea desfășurată în sălile de clasă.

Persoanele cărora li se acordă acces tehnic ori acces la înregistrări răspund pentru păstrarea confidențialității și pentru respectarea limitelor autorizării.

Cuprins

1. Lista responsabililor cu elaborarea, verificarea și aprobarea procedurii
2. Situația edițiilor și a reviziilor
3. Lista de difuzare
4. Scopul procedurii
5. Domeniul de aplicare și documente de referință
6. Definiții și abrevieri
7. Descrierea procedurii
   - 7.1. Principii de bază
   - 7.2. Interdicții exprese privind utilizarea sistemului
   - 7.3. Etapa prealabilă instalării/punerii în funcțiune
   - 7.4. Consultarea, acordul și hotărârea CA
   - 7.5. Informarea persoanelor vizate și semnalizarea
   - 7.6. Amplasarea și funcționarea camerelor
   - 7.7. Vizualizarea în timp real
   - 7.8. Stocarea și ștergerea înregistrărilor
   - 7.9. Accesul la înregistrări
   - 7.10. Cercetarea incidentelor de violență și protecția elevului
   - 7.11. Extragerea și transmiterea înregistrărilor
   - 7.12. Măsuri tehnice și organizatorice de securitate
   - 7.13. Incidente de securitate și încălcări ale datelor
   - 7.14. Drepturile persoanelor vizate
   - 7.15. Revizuirea periodică a necesității monitorizării
8. Responsabilități
9. Formulare
10. Dispoziții finale