



Protocol Cameratoezicht

Versie 2.2 - Datum 02-06-2026

Vastgesteld door HIJN scholengroep:

Versie 2.2 - Datum 02-06-2026 - Jeroen Kwaaitaal - Waarnemend voorzitter college van bestuur HIJN scholengroep

1. Begripsbepalingen

In dit protocol wordt verstaan onder:

- a) Cameratoezicht: toezicht met behulp van camera's, waardoor er sprake is van verwerking van persoonsgegevens als bedoeld in de AVG.
- b) Heimelijk cameratoezicht: cameratoezicht met behulp van verborgen of niet-zichtbare camera's, of cameratoezicht dat niet kenbaar is gemaakt aan betrokkenen.
- c) Camerasysteem: het geheel van camera's, monitoren, opnameapparatuur, verbindingen, software en bevestigingen waarmee het cameratoezicht wordt uitgevoerd, als onderdeel van de ICT-infrastructuur van de scholengroep.
- d) Camerabeeld: het door het cameratoezicht verkregen beeld.
- e) Verwerkingsactiviteit: een handeling met camerabeelden, te onderscheiden in: live uitkijken, opnemen, terugkijken van opgenomen beelden, veiligstellen van beelden bij incidenten en interne inzage.
- f) Inzage: het kennismaken van camerabeelden zonder dat een kopie het camerasysteem verlaat.
Inzage kan plaatsvinden door bevoegde medewerkers van de scholengroep (live uitkijken, terugkijken, interne inzage) of door derden onder de voorwaarden van artikel 9 en betrokkenen onder de voorwaarden van artikel 10.
- g) Interne inzage: het in een beveiligde omgeving ter inzage aanbieden van camerabeelden aan medewerkers van de scholengroep die niet als bevoegde medewerker zijn aangewezen, zonder dat beelden worden gekopieerd of het camerasysteem verlaten.
- h) Uitgifte: het kopiëren van camerabeelden naar een ander medium of het verstrekken van een kopie aan een ontvanger.
Uitgifte vindt plaats onder de voorwaarden van artikel 9 (verstrekking aan derden) of artikel 10 (verzoek om kopie door betrokkene) en is geen zelfstandige verwerkingsactiviteit.
- i) Proceseigenaar: de door het CvB per locatie aangewezen functionaris (standaard de rector/directeur) die verantwoordelijk is voor de naleving van dit protocol op de betreffende locatie.
- j) Operationeel beheerder: de door de proceseigenaar aangewezen persoon die op de locatie het dagelijks camerabeheer coördineert.
- k) Bevoegde medewerker: een door de proceseigenaar aangewezen persoon die bevoegd is tot het uitvoeren van een of meer verwerkingsactiviteiten.
- l) Cameraregister: het overzicht per locatie van alle geplaatste camera's, met per camera het doel, de verwerkingsactiviteiten en de bewaartermijn.
- m) Bevoegdhedenregister: het centraal bijgehouden overzicht van alle personen die zijn aangewezen als proceseigenaar, operationeel beheerder of bevoegde medewerker, met vermelding van hun bevoegdheden.
- n) Incident: een waargenomen ongewenst of strafbaar feit, ongeval of andere gebeurtenis die vraagt om handhaving, onderzoek of strafrechtelijke vervolging.

Voor overige begrippen (waaronder AVG, persoonsgegevens, betrokkene, DPIA, datalek en FG) wordt verwezen naar de definitielijst van het IBP-beleid van HIJN scholengroep.

2. Reikwijdte en verhouding tot overig beleid

- 1. Dit protocol is de operationele uitwerking van het Beleid Beeldmateriaal van HIJN scholengroep (sectie 3.2, Cameratoezicht) en wordt beheerst door het IBP-beleid. De rechtsgrondslag en belangenafweging voor cameratoezicht zijn vastgelegd in het Beleid Beeldmateriaal en het verwerkingsregister.
- 2. Dit protocol geldt voor alle locaties van Stichting HIJN scholengroep waar cameratoezicht wordt ingezet en is van toepassing op alle betrokkenen: leerlingen, hun wettelijk vertegenwoordigers, medewerkers en bezoekers.
- 3. Bij strijdigheid tussen dit protocol en het IBP-beleid of het Beleid Beeldmateriaal, prevaleert het bovenliggende document.

3. Doelstellingen en toegestane verwerkingsactiviteiten

1. Cameratoezicht en het gebruik van camerabeelden is uitsluitend toegestaan voor de volgende doelen:
 - a. de bescherming van de veiligheid en gezondheid van leerlingen, medewerkers en bezoekers;
 - b. de beveiliging van de toegang tot gebouwen en terreinen, waaronder het weren van ongewenste bezoekers;
 - c. de bewaking van zaken die zich in gebouwen of op terreinen bevinden;
 - d. het vastleggen van incidenten.
2. Per doel zijn de volgende verwerkingsactiviteiten toegestaan, mits aan de in dit protocol gestelde voorwaarden is voldaan:

Doel	Live uitkijken	Opnemen	Terugkijken	Interne inzage
a. Veiligheid en gezondheid	Nee	Ja	Ja, bij concrete aanleiding	Ja, bij concrete aanleiding
b. Toegangs-beveiliging	Ja	Ja	Ja, bij concrete aanleiding	Ja, bij concrete aanleiding
c. Bewaking eigendommen buiten reguliere opening	Enkel bij alarmmelding	Ja	Ja, bij concrete aanleiding	Ja, bij concrete aanleiding
d. Vastleggen incidenten	Nee	Ja	Ja, bij gemeld incident	Ja, bij gemeld incident

3. Camerabeelden worden niet voor andere doeleinden gebruikt dan waarvoor zij zijn verzameld. Gebruik voor een ander doel is uitsluitend toegestaan indien dit verenigbaar is met het oorspronkelijke doel en voldoet aan de voorwaarden van artikel 6 lid 4 AVG.
4. Cameratoezicht wordt niet ingezet in ruimtes waar betrokkenen een verhoogde privacyverwachting hebben, waaronder lokalen, kantoren, sanitaire voorzieningen en kleedruimtes.
5. Het cameratoezicht is niet gericht op het verwerken van bijzondere categorieën van persoonsgegevens als bedoeld in artikel 9 AVG; onvermijdelijke incidentele vastlegging wordt in de DPIA geadresseerd.

4. Governance en rollen

1. Het cameratoezicht vindt plaats onder eindverantwoordelijkheid van het College van Bestuur, volgens het Three Lines of Defense-model uit het IBP-beleid.
2. De rolverdeling is als volgt:

Eerste lijn — uitvoering:

Rol	Verantwoordelijkheden
Proceseigenaar (rector/directeur)	Naleving protocol op locatie; aanwijzen operationeel beheerder en bevoegde medewerkers; autoriseren uitgifte van beelden; jaarlijkse rapportage aan CvB
Operationeel beheerder	Dagelijks camerabeheer op locatie; bijhouden cameraregister; aanspreekpunt operationele vragen; faciliteren terugkijksessies en inzageverzoeken; zorgdragen voor kenbaarheid (waarschuwborden)
Bevoegde medewerkers	Uitvoeren en registreren van toegewezen verwerkingsactiviteiten;

Tweede lijn — kaderstelling en monitoring:

Rol	Verantwoordelijkheden
Privacy Officer	Coördineren DPIA's; beheren bevoegdhedenregister; beoordelen inzage- en verwijderingsverzoeken; beoordelen en registreren uitgifte; steekproefcontrole op terugkijklogging
Hoofd ICT	Technische inrichting, beveiliging en beheer camerasysteem; technische toegangscontrole en logging; stellen technische eisen aan hardware en software, leveranciersbeheer
Informatiemanager	Bewaken procesmatige beveiliging; betrokken bij evaluatie en herziening protocol

Derde lijn — onafhankelijk toezicht:

Rol	Verantwoordelijkheden
Functionaris Gegevensbescherming	Onafhankelijk toezicht op naleving; adviseren bij DPIA's en heimelijk cameratoezicht; beoordelen datalekken voor melding bij AP

3. Het CvB wijst per locatie een proceseigenaar aan. Standaard is dit de rector/directeur van de betreffende school.
4. De proceseigenaar wijst voor de eigen locatie een operationeel beheerder en bevoegde medewerkers aan. Het aantal wordt beperkt tot wat noodzakelijk is voor de operationele uitvoering i.v.m. de gevoeligheid van de verwerkingen.
5. De proceseigenaar draagt er zorg voor dat de operationeel beheerder en bevoegde medewerkers voorafgaand aan de uitoefening van hun taken aantoonbaar zijn geïnstrueerd over de werking van het camerasysteem, de kaders van dit protocol en de toepasselijke privacywetgeving. Daarbij moeten zij aantoonbaar een rol spelen in het onderliggende proces.
6. De proceseigenaar wijst voor de operationeel beheerder een plaatsvervanger aan.
7. Waar dit protocol taken toekent aan het Hoofd ICT, kunnen deze worden uitgevoerd door medewerkers van de ICT-afdeling onder verantwoordelijkheid van het Hoofd ICT, tenzij in dit protocol uitdrukkelijk anders is bepaald.
8. Alle aanwijzingen worden vastgelegd in het bevoegdhedenregister. De Privacy Officer beheert dit register en ziet toe op volledigheid en actualiteit. Het bevoegdhedenregister wordt ten minste halfjaarlijks gereviewd door de Privacy Officer in samenwerking met de operationeel beheerders en Hoofd ICT. Bij wijziging van dienstverband, functie, locatie of taakgebied van een rolhouder worden de bijbehorende bevoegdheden binnen vijf werkdagen ingetrokken of aangepast. Rechten in het camerasysteem worden enkel verstrekt op basis van registraties in het register.

5. Besluitvorming en DPIA

1. Het CvB besluit over het instellen, intensiveren of beëindigen van cameratoezicht op een locatie, na advisering door de tweede lijn.
2. Voorafgaand aan een besluit tot het instellen, wijzigen of intensiveren van cameratoezicht wordt de Privacy Officer geraadpleegd en wordt een DPIA uitgevoerd of geactualiseerd. De Privacy Officer coördineert de DPIA in afstemming met het IBP-team, waarbij de FG adviseert conform artikel 35 lid 2 AVG.
3. In de DPIA wordt in ieder geval beoordeeld:
 - a. of het beoogde doel ook met minder ingrijpende middelen kan worden bereikt;
 - b. welke verwerkingsactiviteiten noodzakelijk zijn;
 - c. welke technische en organisatorische waarborgen worden getroffen;
 - d. wat de gevolgen zijn voor de rechten en vrijheden van betrokkenen, in het bijzonder minderjarige leerlingen.
4. Het CvB vraagt de GMR om instemming voorafgaand aan het besluit tot het instellen of wezenlijk wijzigen van cameratoezicht.
5. Besluiten, de DPIA en de instemming van de GMR worden gedocumenteerd en tot 5 jaar na de beëindiging van cameratoezicht bewaard.

6. Inrichting camerasysteem en beveiliging

1. Het Hoofd ICT is verantwoordelijk voor de technische inrichting en het beheer van het camerasysteem, binnen de kaders van de DPIA en de technische beveiligingsstandaarden van de scholengroep.
2. De operationeel beheerder is verantwoordelijk voor de plaatsing en het fysieke onderhoud van camera's op de locatie, conform de specificaties van het Hoofd ICT en binnen de kaders van de DPIA.
3. Het camerasysteem wordt zodanig ingericht dat:
 - a. toegang tot camerabeelden is beperkt tot bevoegde personen, op basis van persoonlijke authenticatie;
 - b. verwerkingsactiviteiten worden automatisch worden gelogd (wie, wanneer, welke camera, welke tijdspanne);
 - c. opgenomen camerabeelden na uiterlijk vier weken automatisch worden gewist;
 - d. standaardinstellingen de gegevensverwerking minimaliseren en niet-noodzakelijke functionaliteiten zijn uitgeschakeld;
 - e. de beveiliging een passend niveau heeft gelet op de risico's, conform artikel 32 AVG.
4. De integriteit van de logging als bedoeld in lid 3 wordt geborgd doordat:
 - a) het aantal accounts met onbegrensde beheerrechten op het camerasysteem wordt beperkt tot een operationeel minimum en deze accounts in het bevoegdhedenregister expliciet als zodanig worden aangewezen;
 - b) functiescheiding wordt aangehouden: een persoon met onbegrensde beheerrechten op het camerasysteem oefent niet tevens de rol van Privacy Officer of Functionaris Gegevensbescherming uit;
 - c) wijzigingen in de samenstelling van accounts met onbegrensde beheerrechten worden vastgelegd in het bevoegdhedenregister en opgenomen in de jaarlijkse rapportage als bedoeld in artikel 13.
5. Toegang tot het camerasysteem op afstand, is uitsluitend toegestaan voor rolhouders aan wie deze toegang in het bevoegdhedenregister expliciet is toegekend, en onder de volgende voorwaarden:
 - a) meervoudige authenticatie is verplicht;
 - b) toegang vindt plaats vanaf door de school beheerde apparatuur, tenzij het Hoofd ICT en de Privacy Officer vooraf instemmen met gebruik van persoonlijke apparatuur en daarbij aanvullende waarborgen vaststellen;
 - c) het Hoofd ICT toetst de inrichting van de remote toegang ten minste jaarlijks.

6. Tijdens schoolvakanties waarin het gebouw niet in regulier gebruik is, wordt de bewaartermijn voor camera's die zijn ingericht voor de doelen toegangsbeveiliging en bewaking van eigendommen verlengd, zodat de beelden van de volledige vakantieperiode beschikbaar blijven tot uiterlijk 7 werkdagen na hervatting van het reguliere gebruik. Hoofd ICT voert het verlengen handmatig door en zet de bewaartermijn binnen 7 werkdagen na hervatting van het reguliere gebruik terug naar de standaardtermijn van vier weken.
7. Geluidsopname is niet toegestaan in het kader van dit protocol. De audiofunctionaliteit van camera's wordt standaard uitgeschakeld. De doelen van het cameratoezicht zoals geformuleerd in artikel 3 vereisen geen audio-opname; visuele beelden volstaan. Het Hoofd ICT ziet erop toe dat bij aanschaf, vervanging en configuratie van camera's de audiofunctie is gedeactiveerd.
8. Opgenomen camerabeelden die samenhangen met een incident worden bewaard zolang de afhandeling van het incident dit noodzakelijk maakt. De proceseigenaar besluit over verlenging van de bewaartermijn en legt de reden en de duur vast. Na afhandeling worden de beelden en eventuele kopieën gewist.
9. Per locatie wordt een cameraregister bijgehouden door de operationeel beheerder, volgens een door het Hoofd ICT en de Privacy Officer vastgesteld format in een daarvoor ingericht systeem. Het register bevat per camera ten minste: locatie, type, doel, verwerkingsactiviteiten en bewaartermijn.
10. Bewerking van camerabeelden is uitsluitend toegestaan voor het verscherpen van beelden of het onherkenbaar maken van personen en valt onder verantwoordelijkheid van Hoofd ICT.
11. Privacy Officer voert steekproefcontrole uit m.b.t. doelmatige inzet van het camerasysteem door logging en registraties kruislings te vergelijken. Indien er onregelmatigheden zijn worden deze besproken met de medewerker.

7. Transparantie en informatieverstrekking

1. De operationeel beheerder draagt er zorg voor dat het cameratoezicht kenbaar wordt gemaakt aan betrokkenen met een gelaagd informatiemodel.
2. Eerste informatielaag (waarschuwbord): Bij elke ingang van gebouwen en terreinen waar cameratoezicht plaatsvindt, wordt een waarschuwbord geplaatst dat ten minste vermeldt wat staat gespecificeerd in bijlage B.
3. Tweede informatielaag: De volledige informatie conform artikel 13 AVG wordt beschikbaar gesteld via de website van de scholengroep en in fysieke vorm op elke locatie. De eerste informatielaag verwijst hiernaar middels een URL of QR-code.
4. De scholengroep hanteert een uniform format voor waarschuwborden op alle locaties.

8. Verwerkingsactiviteiten

Live uitkijken

1. Live uitkijken is uitsluitend toegestaan ten behoeve van toegangsbeveiliging als bedoeld in artikel 3 lid 1 sub b, en bij een alarmmelding buiten reguliere openstellingstijden tevens ten behoeve van bewaking van eigendommen als bedoeld in artikel 3 lid 1 sub c. Het is voorbehouden aan de operationeel beheerder en daartoe aangewezen bevoegde medewerkers.
2. Live uitkijken vindt uitsluitend plaats op camera's die voor de genoemde doelen zijn ingericht en als zodanig zijn opgenomen in het cameraregister.
3. Waar live camerabeelden worden bekeken worden technische en organisatorische maatregelen getroffen die onbevoegd meekijken zo veel als redelijkerwijs mogelijk voorkomen.
4. Indien van toepassing registreert de bevoegde medewerker de alarmmelding die aanleiding gaf tot het live uitkijken, conform het registratiekanaal als bedoeld bij Terugkijken.

Terugkijken

5. Terugkijken is voorbehouden aan de operationeel beheerder en daartoe aangewezen bevoegde medewerkers, en vindt uitsluitend plaats bij een concrete aanleiding die past binnen de doelen van artikel 3 lid 2. Bij uitzondering of onvoldoende capaciteit kan het Hoofd ICT dit faciliteren.
6. Voorafgaand aan elke terugkijksessie registreert de bevoegde medewerker in het daartoe aangewezen registratiekanaal de aanleiding en het tijdsbestek waarop de sessie betrekking heeft. Het registratiekanaal wordt centraal vastgesteld door de Privacy Officer en het Hoofd ICT.
7. De bevoegde medewerker beëindigt de terugkijksessie zodra het doel van de sessie is bereikt.

Veiligstellen bij incidenten

8. Bij een gemeld incident kan Hoofd ICT de relevante camerabeelden markeren ter veiligstelling, waardoor de automatische wissing wordt opgeschort. De veiligstelling wordt gelogd met vermelding van de aanleiding.
9. Toegang tot veiliggestelde fragmenten wordt afzonderlijk toegekend in het bevoegdhedenregister en is niet automatisch verbonden aan andere bevoegdheden binnen het camerasysteem.
10. Na afhandeling van het incident worden veiliggestelde fragmenten verwijderd, conform het besluit van de proceseigenaar als bedoeld in artikel 6 lid 8.

Interne inzage

11. Schoolleiders, afdelingsleiders en leerlingcoördinatoren kunnen bij een concrete aanleiding camerabeelden bekijken ten behoeve van de afhandeling van incidenten. Dit geschiedt altijd in aanwezigheid van een bevoegde medewerker of de operationeel beheerder.
12. Indien beelden op een later moment of door meerdere betrokken medewerkers moeten worden bekeken, stelt het Hoofd ICT deze beschikbaar zodanig dat beelden uitsluitend kunnen worden bekeken en niet kunnen worden gedownload of op andere wijze uit het systeem worden gehaald.
13. Bij interne inzage wordt elke sessie gelogd (wie, wanneer, welke beelden, welke aanleiding).
14. Indien een medewerker buiten de in lid 11 genoemde functies toegang tot camerabeelden nodig heeft, beoordeelt de Privacy Officer vooraf de noodzaak en proportionaliteit. Indien andere betrokkenen (leerlingen, bezoekers, etc.) inzage verzoeken kan dit via de werkwijze beschreven in Artikel 10.

9. Inzage of uitgifte aan derden

Algemeen

1. Inzage en uitgifte van camerabeelden aan derden vindt uitsluitend plaats onder de voorwaarden van dit artikel. Onder derden wordt in dit artikel verstaan: politie, rechter-commissaris, (hulp)officier van justitie en overige externe partijen. Verzoeken van betrokkenen tot inzage in of verstrekking van een kopie van beelden waarop zij zelf herkenbaar voorkomen, worden behandeld conform artikel 10.
2. Op verzoek van politie, rechter-commissaris of (hulp)officier van justitie kan inzage of uitgifte plaatsvinden in het kader van de uitoefening van hun publiekrechtelijke taak, onder de voorwaarden van dit artikel.
3. Aan overige derden vindt geen inzage of uitgifte plaats, tenzij met uitdrukkelijke toestemming van de betrokkene(n) die op de beelden herkenbaar zijn.
4. De Privacy Officer beoordeelt voorafgaand aan elke inzage of uitgifte of deze rechtmatig is, op basis van de aanleiding en het door de verzoekende partij aangegeven doel. Bij twijfel wordt de FG geraadpleegd.
5. Inzage en uitgifte blijven beperkt tot het tijdsbestek en de camera's die voor de aanleiding relevant zijn.
6. Alvorens tot inzage of uitgifte over te gaan, legitimeert de verzoekende functionaris zich ten overstaan van een bevoegd medewerker.
7. De Privacy Officer registreert elke inzage en elke verstrekking als bedoeld in dit artikel.

Inzage

8. Inzage vindt plaats onder begeleiding van de operationeel beheerder of een bevoegde medewerker. Onherkenbaar maken van overige betrokkenen voorafgaand aan inzage is niet vereist, omdat de inzage binnen de begrenzing van lid 5 plaatsvindt.

Uitgifte

9. Uitgifte van camerabeelden aan deze partijen vindt uitsluitend plaats op een formele vordering. Bij een vordering is medewerking verplicht; de proceseigenaar wordt geïnformeerd.
10. Uitgifte geschiedt uitsluitend door of onder verantwoordelijkheid van het Hoofd ICT. De ontvanger tekent voor ontvangst.
11. Voorafgaand aan uitgifte worden overige betrokkenen die herkenbaar voorkomen op de beelden onherkenbaar gemaakt, tenzij dit technisch niet mogelijk is of de aard van de aanleiding zich daartegen verzet.
12. Bij uitgifte wordt vastgelegd: de aanleiding, het doel, de ontvanger, de datum, de omvang van de verstrekte beelden en eventuele voorwaarden.

10. Rechten van betrokkenen

1. Betrokkenen kunnen de rechten uitoefenen die de AVG hen toekent, waaronder het recht op inzage, beperking, verwijdering, rectificatie en bezwaar.
2. Een verzoek tot uitoefening van rechten met betrekking tot camerabeelden wordt ingediend via ibp@hijnscholengroep.nl of schriftelijk bij de operationeel beheerder van de betreffende locatie. De operationeel beheerder stuurt het verzoek onverwijld door aan de Privacy Officer.
3. De Privacy Officer beoordeelt het verzoek en draagt zorg voor een eerste inhoudelijke reactie binnen 10 werkdagen na ontvangst. Het verzoek wordt afgehandeld binnen de termijn van artikel 12 AVG.
4. Bij een inzageverzoek specificeert de betrokkene zo nauwkeurig mogelijk wanneer en waar hij of zij zich in het bewaakte gebied bevond. De Privacy Officer informeert de betrokkene vooraf welke informatie nodig is om het verzoek te kunnen behandelen.
5. Inzage vindt primair plaats op de locatie, in aanwezigheid van de operationeel beheerder of een bevoegde medewerker. Waar nodig worden andere betrokkenen onherkenbaar gemaakt voorafgaand aan de inzage.

6. Wanneer de betrokkene expliciet verzoekt om een kopie van de beelden (artikel 15 lid 3 AVG), vindt uitgifte plaats onder de procedurele waarborgen van artikel 9 (uitgifte). De Privacy Officer toetst daarbij in het bijzonder of de rechten en vrijheden van andere betrokkenen op de beelden zijn gewaarborgd.
7. Een verzoek wordt afgewezen wanneer het ongespecificeerd is, wanneer er kennelijk misbruik van recht wordt gemaakt, of wanneer het verstrekken van een kopie noodzakelijkerwijs afbreuk doet aan de rechten en vrijheden van anderen en anonimiseren technisch niet mogelijk is. In geval van een lopend incident kan een verzoek worden geweigerd voor zover dit noodzakelijk is in het belang van de voorkoming, opsporing en vervolging van strafbare feiten.
8. Klachten over cameratoezicht worden behandeld conform de klachtenprocedure van Stichting HIJN Scholengroep. Voor klachten over de omgang met persoonsgegevens kan tevens een klacht worden ingediend bij de FG via fg@hijnscholengroep.nl of bij de Autoriteit Persoonsgegevens.

11. Heimelijk cameratoezicht

1. Heimelijk cameratoezicht is uitsluitend toegestaan indien regulier cameratoezicht en andere maatregelen niet hebben geleid tot beëindiging van structurele incidenten. Heimelijk cameratoezicht is niet toegestaan voor preventieve doeleinden.
2. Heimelijk cameratoezicht mag alleen tijdelijk worden ingezet en op zodanige wijze dat de inbreuk op de persoonlijke levenssfeer van betrokkenen zo klein mogelijk is. Inzet in ruimtes als bedoeld in artikel 3 lid 4 is onder geen omstandigheid toegestaan.
3. Voorafgaand aan inzet van heimelijk cameratoezicht:
 - a. voert de Privacy Officer een afzonderlijke DPIA uit, de DPIA richt zich specifiek op de voorgenomen heimelijke inzet en adresseert in het bijzonder welke andere maatregelen zijn geprobeerd en waarom die niet hebben geleid tot beëindiging van de structurele incidenten, de afbakening in tijd, plaats en doelgroep, en de wijze waarop betrokkenen achteraf worden geïnformeerd;
 - b. adviseert de FG over de voorgenomen verwerking;
 - c. verleent het CvB schriftelijke toestemming, onder vermelding van het doel, de locatie, de duur en de voorwaarden.
4. Het CvB informeert de GMR onverwijld na beëindiging van het heimelijk cameratoezicht over de inzet, de aanleiding en de uitkomsten, voor zover dit niet in strijd is met lopend onderzoek door politie of justitie. Indien het heimelijk cameratoezicht langer duurt dan vier weken, wordt de GMR tussentijds onder geheimhouding geïnformeerd.
5. Na afloop van het heimelijk cameratoezicht informeert de scholengroep - voor zover redelijkerwijs mogelijk - de betrokkenen achteraf over het toegepaste toezicht.

12. Incidenten en datalekken

1. Bij een beveiligingsincident of vermoedelijk datalek met betrekking tot camerabeelden handelt de scholengroep conform het Protocol privacy en datalekken van HIJN scholengroep.
2. De operationeel beheerder meldt incidenten met betrekking tot het camerasysteem onverwijld aan het Hoofd ICT en de Privacy Officer.

13. Verslaglegging, evaluatie en herziening

1. De proceseigenaar rapporteert jaarlijks aan het CvB over het cameratoezicht op de locatie, waaronder:
 - a. het aantal en de aard van terugkijksessies;
 - b. verstrekkingen van beelden aan derden;
 - c. ontvangen verzoeken van betrokkenen;
 - d. incidenten met betrekking tot het camerasysteem;
 - e. een toets op de omvang en effectiviteit.
2. De noodzaak en proportionaliteit van het cameratoezicht wordt minimaal elke twee jaar herbeoordeeld als onderdeel van de planning-en-control cyclus uit het IBP-beleid.
3. Dit protocol wordt minimaal elke twee jaar geëvalueerd en indien nodig herzien, gelijktijdig met de evaluatie van het IBP-beleid en het beleid Beeldmateriaal.

14. Slotbepalingen

1. Het College van Bestuur stelt dit protocol vast. Voorafgaand aan het vaststellen, wezenlijk wijzigen of intrekken van dit protocol vraagt het CvB de GMR om instemming.
 2. Het CvB informeert, indien aanwezig, de leerlingenraad over het vaststellen, wezenlijk wijzigen of intrekken van dit protocol.
 3. Dit protocol treedt in werking op de datum van vaststelling. Wijzigingen treden in werking binnen 30 dagen na bekendmaking.
-

Bijlage A — Template cameraregister

Per locatie registreren we per camera de volgende zaken:

Veld	Toelichting
Camera-ID	Uniek nummer per camera
Locatie	Gebouw, verdieping, positie
Type	Vast / draaibaar
Doel(en)	Verwijzing naar artikel 3 lid 1 sub a t/m d
Verwerkingsactiviteiten	Live uitkijken toegangsbeveiliging / Live uitkijken alarmmelding / opname [meerkeuze]
Bewaartermijn	Standaard: 4 weken, of specifieke termijn met onderbouwing
Datum plaatsing	
Datum laatste herziening	

Bijlage B — Richtlijnen waarschuwbord (eerste informatielaag)

Uniform format voor alle locaties wordt door communicatie verzorgd.

Het waarschuwbord bevat ten minste:

1. **Pictogram:** camerabewaking
2. **Verwerkingsverantwoordelijke:** Stichting HIJN Scholengroep
3. **Contact:** ibp@hijnscholengroep.nl
4. **Meer informatie:** [URL schoolwebsite] en/of QR-code
5. **Plaatsing:** bij elke ingang, op ooghoogte, voordat de betrokkene het bewaakte gebied betreedt.

Bijlage C — Template bevoegdhedenregister

Per locatie registreren we per bevoegde medewerker de volgende zaken:

Veld	Toelichting
Naam	
Functie	
Locatie	
Rol	Proceseigenaar / operationeel beheerder / bevoegde medewerker / Incidentafhandeling / Onbegrensd beheer
Bevoegde	
Verwerkingsactiviteiten	Live uitkijken toegangsbeveiliging / Live uitkijken alarmmelding / terugkijken / uitgeven
Plaatsvervanger van	Indien van toepassing
Datum aanwijzing	
Aangewezen door	Naam proceseigenaar of CvB
Datum beëindiging	Indien van toepassing