

Reglement Cameratoezicht OMO

Vastgestelde versie 8 juli 2025

Bron: Gebaseerd op het ModelReglement cameratoezicht FSR (MBO Raad) 2020 bewerkt door het Summa College (2025) en aangepast voor OMO (2025)

Inhoud

1. Inleiding	3
2. Definities en reikwijdte	5
2.1 Definities	5
2.2 Reikwijdte en werkingssfeer	6
3. Cameratoezicht	7
3.1 Doelen van het cameratoezicht	7
3.2 Taken en verantwoordelijkheden	7
3.3 Inrichten Camerasysteem en beveiliging	8
3.4 Het plaatsen van camera's	9
3.5 Privacy en rechten van betrokkenen	9
3.6 Inzage en uitgifte opgenomen Camerabeelden aan derden	10
3.7 Heimelijk Cameratoezicht	11
3.8 Verslaglegging en rapportage	11
4. Klachten	12
5. Slotbepalingen	13
BIJLAGEN	14

1. Inleiding

Cameratoezicht, ook wel bekend onder het Engelse begrip CCTV, wordt in verschillende situaties gebruikt, bijvoorbeeld om personen en eigendommen te beschermen. Gemeentes gebruiken cameratoezicht bijvoorbeeld in het kader van veiligheid op straat. Het is hierbij van belang dat organisaties zorgvuldig met camerabeelden omgaan. Ook onderwijsinstellingen maken gebruik van cameratoezicht.

Het inzetten van cameratoezicht wordt toegepast om de veiligheid van medewerkers, leerlingen en bezoekers binnen en in de directe omgeving van locaties van scholen te waarborgen. Cameratoezicht mag geen doel op zichzelf zijn. Het maakt deel uit van een totaalpakket aan maatregelen rondom beveiliging en sociale veiligheid binnen een school. Vanuit haar eigen visie op samenwerken vanuit aandacht, begeleiding en vertrouwen, en de grote impact van cameratoezicht op de privacy van leerlingen en medewerkers, ziet OMO Cameratoezicht als een zwaar middel dat slechts met de nodige terughoudendheid ingezet mag te worden.

Bij OMO kunnen camera's worden ingezet in het kader van toezicht, bijvoorbeeld om vernielingen of diefstal tegen te gaan. De afweging hoeveel cameratoezicht gewenst is, verschilt per locatie. Het Reglement biedt kaders om deze afweging te maken.

Omdat er bij cameratoezicht sprake is van een inbreuk op de privacy van medewerkers, leerlingen en bezoekers, moet het cameratoezicht aan een aantal voorwaarden voldoen. Door cameratoezicht kan het gedrag van leerlingen en medewerkers worden gevolgd. De inbreuk op de privacy moet zo klein mogelijk zijn. Het uitgangspunt blijft dat mensen onbevangen zichzelf moeten kunnen zijn. Bijvoorbeeld een camera ophangen in kleedruimtes gaat te ver, omdat mensen dan ontkleed in beeld kunnen komen.

Toepassingsbereik

Dit Reglement betreft uitsluitend cameratoezicht voor doeleinden als bovengenoemd. Het gaat met name om toezicht voor de veiligheid in de gebouwen en op de terreinen en de beveiliging van onze eigendommen.

Overigens worden camera's ook gebruikt tijdens het onderwijs, bijvoorbeeld in het kader van les op afstand of voor beeldcoaching. Daarnaast wordt vaak beeldmateriaal gemaakt van evenementen. Voor deze andere vormen van cameragebruik dan cameratoezicht gelden andere kaders, neergelegd in desbetreffende beleidsstukken, richtlijnen en werkafspraken.

Dit Reglement geeft aan welke taken, verantwoordelijkheden en procedures gelden bij cameratoezicht. Met behulp daarvan kan OMO het cameratoezicht effectief, efficiënt en verantwoord inzetten, waar dat aantoonbaar bijdraagt aan de veiligheid. Het doel van dit Reglement is een integer gebruik van cameratoezicht en de bescherming van privacy van leerlingen, medewerkers en bezoekers te borgen.

Verantwoordelijkheid

Het zorgvuldig omgaan met persoonsgegevens is (wettelijk) de verantwoordelijkheid van de Raad van Bestuur.

In dit Reglement is beschreven dat de verantwoordelijkheid voor het uitvoeren van het cameratoezicht (beheer) is gemandateerd aan een door de directeur van het OMO-Bureau aan te wijzen functionaris, in dit document de Beheerder genoemd. Op scholen en alle overige locaties zijn Locatiebeheerders verantwoordelijk voor de uitvoering van het Cameratoezicht. Zij worden aangewezen door de locatieverantwoordelijke rector/directeur. De Locatiebeheerders rapporteren aan de Beheerder over het uitgevoerde Cameratoezicht. De Teamleider IT van het OMO-Bureau is belast met het Technisch beheer.

De Raad van Bestuur blijft eindverantwoordelijk voor het toepassen van Cameratoezicht.

Dit Reglement is op 8 juli 2025 door de Raad van Bestuur vastgesteld na instemming van de Gemeenschappelijke Medezeggenschapsraad (GMR).

2. Definities en reikwijdte

2.1 Definities

In dit Reglement worden de volgende definities gebruikt:

1. AVG: Algemene Verordening Gegevensbescherming.
2. Beheer: de zorg voor de uitvoering en continuïteit van het Cameratoezicht.
3. Beheerder: de door de directeur van het OMO-Bureau aangewezen functionaris die verantwoordelijk is voor het Beheer.
4. Betrokkene: degene die wordt geregistreerd door het camerasysteem, oftewel een leerling, medewerker of bezoeker van een locatie.
5. Bevoegde medewerker: de door de Beheerder of de Locatiebeheerder geautoriseerde medewerker die onder diens verantwoordelijkheid Camerabeelden mag bekijken.
6. Camerabeeld(en) (beeldinformatie): de door camera's en/of het Camerasysteem verkregen beelden in *real time* en opgenomen of geregistreerde beelden.
7. Cameraobservatieruimte: een ten behoeve van Cameratoezicht centraal gesitueerde, van een toegangscontrolesysteem voorziene ruimte, waarin de camerabeelden – van een of meer locaties - live worden bekeken en/of waar ook de mogelijkheid bestaat om opgenomen camerabeelden terug te kijken en/of op een informatiedrager te plaatsen.
8. Camerasysteem: het geheel van camera's, monitoren, opnameapparatuur, verbindingkasten en verbindingen waarmee het cameratoezicht wordt uitgevoerd.
9. Cameratoezicht: toezicht met behulp van camera's, waardoor er sprake is van verwerking van persoonsgegevens als bedoeld in de AVG.
10. Raad van Bestuur: het bestuur als bedoeld in de statuten van OMO;
11. Functionaris voor gegevensbescherming: de in de AVG bedoelde en door de Raad van Bestuur aangewezen interne toezichthouder voor privacy.
12. Heimelijk cameratoezicht: tijdelijk ingezet toezicht met behulp van verborgen en/of niet-zichtbare camera's, of toezicht met camera's dat niet kenbaar is gemaakt aan leerlingen, medewerkers en bezoekers.
13. Incident: een (vermoeden van een) waargenomen ongewenst en/of strafbaar feit, ongeval of andere gebeurtenis die vraagt om handhaving, onderzoek en/of aangifte bij de politie.
14. Locatie: een gebouw of terrein waar OMO Cameratoezicht toepast.
15. Locatiebeheerder: een door locatieverantwoordelijke rector of directeur als zodanig aangewezen medewerker die belast is met het Cameratoezicht op één of meerdere locaties van het OMO en daarover verantwoording aflegt aan de Beheerder.
16. Serverruimte: de van een toegangscontrolesysteem voorziene ruimte, waar de server of opnameapparatuur staat waarop de opgenomen camerabeelden geregistreerd staan.
17. OMO: de Vereniging Ons Middelbaar Onderwijs en de scholen die onder dit bestuur vallen;
18. Privacy Officer: de medewerker als bedoeld in het OMO informatiebeveiligings- en privacybeleid en als tweedelijns functionaris belast met het ontwikkelen en implementeren van het privacybeleid;
19. Security Officer: de medewerker als bedoeld in het OMO informatiebeveiligings- en privacybeleid en als tweedelijns functionaris onder meer belast met het ontwikkelen en implementeren van het informatiebeveiligingsbeleid;

20. Technisch beheerder: de Teamleider IT (OMO Bureau), door de Raad van Bestuur belast met het technisch beheer van het Camerasysteem.
21. Technisch medewerker: de door de Technisch beheerder aangewezen medewerker die belast is met het uitvoeren van technisch beheer van het Camerasysteem.
22. Verwerker: het bedrijf dat of de organisatie die door het OMO is ingeschakeld om (een deel van) het Cameratoezicht te verzorgen.

2.2 Reikwijdte en werkingssfeer

1. Het Reglement Cameratoezicht OMO 2025 (hierna: het/dit Reglement) heeft betrekking op alle locaties van het OMO waar Cameratoezicht wordt ingezet.
2. Dit Reglement is van toepassing op leerlingen, medewerkers en bezoekers die zich bevinden in de gebouwen of op de terreinen van OMO.
3. In situaties waarin OMO gebruik maakt van locaties van derden, of wanneer derden op locaties van OMO cameratoezicht willen inzetten, ziet OMO erop toe dat het toezicht binnen de kaders van dit Reglement wordt ingezet.
4. Bij het plaatsen van toegangscamera's zorgt OMO ervoor dat deze niet gericht zijn op gebieden buiten het eigen terrein. Indien het onvermijdelijk is dat toezichtcamera's als "bijvangst" ook deels buiten het eigen terrein beelden maken, dan is OMO uiterst terughoudend met het gebruik hiervan.
5. Het Reglement Cameratoezicht OMO 2025 maakt onderdeel uit van het vastgestelde OMO informatiebeveiligings- en privacybeleid.

3. Cameratoezicht

3.1 Doelen van het cameratoezicht

Cameratoezicht wordt *uitsluitend* gebruikt voor de volgende doelen:

1. De bescherming van de veiligheid en gezondheid van leerlingen, medewerkers en bezoekers;
2. De beveiliging van de toegang tot gebouwen en terreinen, waaronder mede begrepen het weren van onbevoegden;
3. Het voorkomen en registreren van overlast en strafbare feiten zoals vandalisme, diefstal en inbraak;
4. De bewaking van zaken die zich in de gebouwen of op de terreinen bevinden;
5. Het vastleggen van incidenten ten aanzien van de in punt 1 t/m 4 genoemde doelen.

3.2 Taken en verantwoordelijkheden

1. De Raad van Bestuur van OMO is Verwerkingsverantwoordelijke in de zin van de AVG.
2. Overeenkomstig het vastgestelde OMO Informatiebeveiligings- en Privacybeleid zijn de rectoren en directeuren binnen de eigen school/organisatieonderdeel verantwoordelijk voor de naleving van de in en bij dit Reglement gestelde kaders.
3. Binnen OMO is de Beheerder verantwoordelijk voor de inrichting, het beheer van en het toezicht op het Cameratoezicht.
4. De Technisch Beheerder ondersteunt de Beheerder met het Technisch beheer van het Camerasysteem.
5. De locatieverantwoordelijke rector/directeur wijst een Locatiebeheerder en diens plaatsvervanger aan, alsmede Bevoegde medewerkers. Deze aanwijzing wordt doorgegeven aan de Beheerder die een overzicht hiervan bijhoudt en actueel houdt.
6. De Beheerder, Locatiebeheerder(s) en Bevoegde medewerkers zijn bevoegd tot het live meekijken en terugkijken van opgenomen camerabeelden.
7. De Beheerder en Locatiebeheerder kunnen medewerkers autoriseren om - onder verantwoordelijkheid van de Beheerder of Locatiebeheerder - onder nader te stellen voorwaarden opgenomen Camerabeelden terug te kijken. Hier kunnen werkinstructies voor worden gegeven door de Beheerder en/of Locatiebeheerder.
8. De Beheerder is verantwoordelijk voor de toegang tot Camerabeelden en ziet erop toe dat alleen Bevoegde medewerkers toegang hebben.
9. De Technisch beheerder is verantwoordelijk voor het technisch beheer van het Camerasysteem en Serverruimte. De Technisch beheerder wijst een of meerdere Technische medewerkers aan. Alleen met toestemming van de Technisch beheerder krijgen derden in het kader van onderhoud en beheer toegang tot het Camerasysteem.
10. Alle met het Cameratoezicht belaste medewerkers gaan vertrouwelijk en integer om met de beeldinformatie, in het bijzonder met betrekking tot de privacy van personen. Toegang tot en gebruik van Camerabeelden valt onder de

arbeidsrechtelijke geheimhouding. Medewerkers ontvangen hierover bij aanvang van de werkzaamheden en vervolgens minimaal jaarlijks instructie.

11. De Locatiebeheerder zorgt voor (integrale en ongewijzigde) publicatie van dit Reglement op de website van iedere school of locatie die onder diens verantwoordelijkheid Cameratoezicht toepast. Voor scholen of locaties zonder Cameratoezicht geldt dat op de website van de betreffende school of locatie gemeld kan worden dat er geen Cameratoezicht plaatsvindt.
12. De Beheerder wint advies in bij de Security Officer en/of de Privacy Officer in gevallen waarvoor het Reglement onvoldoende duidelijkheid geeft.

3.3 Inrichten Camerasysteem en beveiliging

1. De Locatiebeheerder is verantwoordelijk voor de inrichting van het Camerasysteem en de plaatsing van de camera's binnen de kaders van dit Reglement. Plaatsing van camera's vindt plaats in overleg met de locatieverantwoordelijke rector/directeur.
2. De Beheerder ziet in samenspraak met de Technisch Beheerder toe op passende technische en organisatorische maatregelen om de Camerabeelden te beveiligen tegen verlies of tegen enige vorm van onrechtmatig gebruik. Deze maatregelen garanderen, rekening houdend met de stand van de techniek (zoals te doen gebruikelijk in de informatiebeveiligings- en beveiligingsbranche) en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's van het cameratoezicht en de aard van te beschermen Camerabeelden met zich meebrengen. De maatregelen betreffen het Camerasysteem, de Serverruimte en de Cameraobservatieruimte.
3. Het terugkijken van opgenomen Camerabeelden geschiedt in aanwezigheid van ten minste twee personen, onder wie in ieder geval een bevoegde persoon.
4. De gebeurtenissen waarvoor Camerabeelden mogen worden teruggekeken, sluiten aan bij de doelen waarvoor de beelden zijn gemaakt. Bij het besluit om al dan niet beelden terug te kijken, wordt rekening gehouden met de ernst van de situatie.
5. De Beheerder ziet erop toe dat het Cameratoezicht kenbaar wordt gemaakt aan leerlingen, medewerkers en bezoekers op zichtbare en herkenbare wijze, zoals, maar niet beperkt tot, borden en stickers bij de ingang/toegangspunten van de gebouwen of terreinen. De bebording bevat tenminste een pictogram van een camera en de toevoeging cameratoezicht. Bij elke camera is een sticker/waarschuwing aangebracht.
6. Voor zover er in het Camerasysteem Camerabeelden worden opgeslagen, worden deze beelden maximaal vier weken na de opname automatisch gewist, tenzij er een Incident is geconstateerd op basis waarvan het noodzakelijk is de met het Incident samenhangende Camerabeelden te bewaren (veiligstellen). Na afhandeling van het Incident worden de betreffende camerabeelden (en eventueel gemaakte kopieën of afdrukken) gewist.
7. Het Camerasysteem is zodanig uitgerust dat het terugkijken van opgenomen Camerabeelden of het uitgeven daarvan beperkt is tot Bevoegde en Technisch medewerkers.
8. Voor zover er Camerabeelden live worden uitgekeken in een andere ruimte dan de Serverruimte of Cameraobservatieruimte, zijn er maatregelen genomen die het onbevoegd meekijken zoveel als redelijkerwijs mogelijk voorkomen.
9. Meekijken of terugkijken door leerlingen, ongeautoriseerde medewerkers of bezoekers is niet mogelijk, met uitzondering van het terugkijken van beelden waar de betrokkene zelf op staat op grond van een AVG-inzageverzoek.

10. Voor zover er bij het inrichten van het Camerasysteem gekozen wordt om de leerlingen, medewerkers en bezoekers via een monitor live terugkoppeling te geven van de Camerabeelden, kunnen deze live Camerabeelden alleen betrekking hebben op deze betreffende leerlingen, medewerkers en bezoekers.
11. Bewerking van Camerabeelden vindt slechts plaats in het kader van het selecteren of verscherpen van deze Camerabeelden, of ten behoeve van het noodzakelijkerwijs onherkenbaar maken van bepaalde niet-betrokken personen op die Camerabeelden.
12. Het gebruik van gezichtsherkenningsoftware is niet toegestaan. Evenmin is het toegestaan Artificial Intelligence technieken in te zetten bedoeld om gedragingen vast te leggen, te analyseren, te interpreteren of te voorspellen.
13. De Beheerder zorgt voor werkinstructies voor het inzien en uitgeven van Camerabeelden en zorgt dat deze procedures bekend zijn bij de Locatiebeheerders, Bevoegde en Technische medewerkers.

3.4 Het plaatsen van camera's

1. Camera's worden uitsluitend geplaatst en gehandhaafd wanneer dit noodzakelijk is en er geen minder ingrijpende maatregelen dan Cameratoezicht voorhanden zijn om de doelen zoals vermeld in artikel 30, te bereiken. De Locatiebeheerder houdt een overzicht bij van de geplaatste camera's.
2. Het is mogelijk om in afstemming met de Beheerder, naast Camerabeelden, ook geluidsopnames bij dezelfde beelden te maken (video en audio). Het maken van audio-opnames zonder beeld is niet toegestaan. Met het live meekijken van camerabeelden inclusief geluid, wordt terughoudend omgegaan en vraagt aparte motivering en afstemming met de Beheerder en advies van de Functionaris voor Gegevensbescherming.
3. De locatieverantwoordelijke rector/directeur ziet erop toe dat de overwegingen tot plaatsing of handhaving van camera's worden vastgelegd. Jaarlijks beoordeelt de Locatiebeheerder of de noodzaak uit het eerste lid van dit artikel nog steeds van toepassing is.
4. De Locatiebeheerder zorgt ervoor dat een actueel overzicht voorhanden is van in het kader van Cameratoezicht geplaatste camera's en deelt dit met de Beheerder. Wijzigingen worden binnen één maand doorgegeven aan de Beheerder.

3.5 Privacy en rechten van betrokkenen

1. Betrokken leerlingen, medewerkers en bezoekers komen de rechten toe zoals bedoeld in de AVG. Hieronder vallen het recht op inzage, correctie en verwijdering van camerabeelden waarop zij zijn afgebeeld.
2. Een verzoek tot inzage in Camerabeelden geschiedt schriftelijk of per e-mail aan de Beheerder, die binnen een maand na ontvangst van het verzoek inhoudelijk zal reageren. Een elders binnen OMO ontvangen verzoek wordt onmiddellijk doorgezonden naar de Beheerder.
3. De Beheerder wordt bij de behandeling van het verzoek ondersteund door de Security Officer en de Privacy Officer die zonodig het advies van de Functionaris Gegevensbescherming inwinnen.
 De Locatiebeheerder stuurt vervolgens verzoeker schriftelijk of per e-mail de formele reactie op het verzoek.

4. Het verzoek tot inzage wordt afgewezen wanneer het verzoek niet gespecificeerd is, de identiteit van de verzoeker niet vastgesteld kan worden, of als met dit verzoek kennelijk misbruik van recht wordt gemaakt.
5. In geval van een Incident kan een inzageverzoek worden geweigerd als dat noodzakelijk is in het belang van de (verdere) voorkoming, opsporing en vervolging van strafbare feiten.
6. Betrokkenen kunnen ten aanzien van de oefening van hun rechten van betrokken zoals bedoeld in de AVG, zich eveneens wenden tot de Functionaris voor Gegevensbescherming.

3.6 Inzage en uitgifte opgenomen Camerabeelden aan derden

1. Inzage en verstrekking aan derden van met het Camerasysteem opgeslagen beeldinformatie is alleen mogelijk in een van deze gevallen:
 - a. op basis van een wettelijke verplichting;
 - b. bij (vermoeden van) een strafbaar feit en/of (voorgenomen) aangifte daarvoor;
 - c. in andere gevallen als dit verenigbaar is met het bepaalde in de AVG en het doel van het Cameratoezicht zoals vermeld in artikel 0.
2. Op verzoek van politie, rechter-commissaris of (hulp)officier van justitie kan inzage worden gegeven in (opgenomen) Camerabeelden in het kader van de uitoefening van hun publiekrechtelijke taken.
3. Uitgifte van Camerabeelden vindt slechts plaats op vordering van de politie, rechter-commissaris of (hulp)officier van justitie waarbij de vordering gebaseerd is op een wettelijke grondslag. De vordering dient onmiddellijk ter beoordeling te worden doorgezet naar de Beheerder.
4. Alvorens tot inzage of uitgifte over te gaan, legitimeert de betreffende functionaris zich vooraf ten overstaan van de Beheerder of Locatiebeheerder, en deze functionaris tekent voor ontvangst van de uitgegeven Camerabeelden.
5. De inzage en uitgifte wordt voorafgaand afgestemd met de Beheerder of Locatiebeheerder en aansluitend geregistreerd. Bij twijfel wordt overlegd met de Functionaris voor Gegevensbescherming.
6. Een verzoek tot inzage en/of verstrekking van Camerabeelden door een derde (anders dan beschreven in dit artikel) dient schriftelijk of digitaal te worden ingediend bij de Beheerder. Deze beslist, na weging van de belangen en na advies van de Functionaris voor Gegevensbescherming, zo spoedig mogelijk op de aanvraag.
7. Inzage van Camerabeelden door derden vindt altijd plaats in het bijzijn van de Beheerder of een Locatiebeheerder.
8. Het inzien, uitgeven of bewaren van beeldinformatie door derden of naar aanleiding van een Incident wordt vastgelegd in het Incidentenregister. Hierbij wordt ten minste opgenomen op wiens verzoek wordt teruggekeken, de aanleiding tot het verzoek, de reden om toegang te geven, wie de beeldinformatie heeft ingekeken, wat de uitkomst is geweest en aan wie de informatie is verstrekt.

3.7 Heimelijk Cameratoezicht

1. Heimelijk Cameratoezicht is slechts toegestaan indien regulier Cameratoezicht en andere door OMO genomen maatregelen en inspanningen, niet hebben geleid tot beëindiging van een structureel Incident. Heimelijk Cameratoezicht is niet mogelijk voor preventieve doeleinden.
2. Heimelijk Cameratoezicht mag alleen tijdelijk en op zodanige wijze worden ingezet, dat sprake is van een minimale inbreuk op de persoonlijke levenssfeer van leerlingen, medewerkers en bezoekers.
3. Heimelijk Cameratoezicht is uitsluitend toegestaan na een daartoe strekkend specifiek voorafgaand schriftelijk besluit van de Raad van Bestuur op voordracht van de Beheerder en na advies van de Functionaris voor Gegevensbescherming.
4. Een verzoek voor toepassing van heimelijk Cameratoezicht gaat gepaard met een privacytoets (DPIA), met vermelding van de voorwaarden en periode waaronder het heimelijk Cameratoezicht plaatsvindt.
5. De Raad van Bestuur informeert de GMR over de inzet van heimelijk Cameratoezicht. Ingeval voorafgaand informeren redelijkerwijs niet haalbaar is, dan wordt de GMR zo spoedig als mogelijk is op de hoogte gesteld.
6. De Beheerder informeert – voor zover redelijkerwijs mogelijk – achteraf betrokken leerlingen, medewerkers en bezoekers over het toegepaste heimelijk Cameratoezicht.

3.8 Verslaglegging en rapportage

1. De Beheerder doet jaarlijks aan de Raad van Bestuur verslag over het toegepaste Cameratoezicht.
2. Jaarlijks wordt door de Raad van Bestuur gerapporteerd aan de GMR over het Cameratoezicht betreffende het voorafgaande kalenderjaar (over aard, frequentie en lengte van het toezicht). Hierbij wordt specifiek gemeld of ook heimelijk Cameratoezicht is toegepast.

4. Klachten

1. Klachten over Cameratoezicht, over het gedrag van de bij het Cameratoezicht of cameragebruik betrokken medewerkers, dienen schriftelijk of digitaal te worden ingediend bij de Beheerder.
2. Desgewenst kunnen betrokkenen zich voor wat betreft gegevensbeschermingsklachten of -vragen richten tot de Functionaris voor Gegevensbescherming (fg@omo.nl).

5. Slotbepalingen

1. Dit Reglement is na instemming van de GMR vastgesteld door de Raad van Bestuur op 8 juli 2025.
2. Dit Reglement geldt met ingang van 8 juli 2025, waarmee alle voorgaande Reglementen (van OMO of individuele scholen) niet (langer) van toepassing zijn. Vaststelling door individuele rectoren of directeuren is niet nodig.
3. Dit Reglement kan worden aangehaald als "Reglement Cameratoezicht OMO 2025" en wordt gepubliceerd op de publiektoegankelijke intra- en internetpagina's van OMO alsmede alle individuele scholen indien waar Cameratoezicht plaatsvindt.
4. Dit Reglement alsmede de operationele inzet van Cameratoezicht wordt jaarlijks geëvalueerd en zo nodig aangepast.

BIJLAGEN

- A. Juridische randvoorwaarden
- B. Aanwijzing plaatsvervangend Beheerder, Technisch beheerder, Technisch medewerkers
- C. Overzicht camera's t.b.v. Cameratoezicht

BIJLAGE A. Juridische randvoorwaarden

De (Europese) wetgever en gezamenlijke Europese privacy-toezichthouders (EDPB) geven een onderwijsinstellingen een aantal randvoorwaarden mee waar cameratoezicht aan moet voldoen. De toezichthouder in Nederland op het gebruik van persoonsgegevens, de Autoriteit Persoonsgegevens, heeft dit uitgewerkt in haar beleidsregels.

Cameratoezicht en cameragebruik wordt getoetst aan deze juridische randvoorwaarden.

1. Gerechtvaardigd belang

OMO moet een zogeheten gerechtvaardigd belang hebben voor het cameratoezicht. Bijvoorbeeld diefstal tegengaan of de sociale en fysieke veiligheid van leerlingen, medewerkers en bezoekers beschermen.

2. Noodzaak cameratoezicht

Het cameratoezicht moet noodzakelijk zijn. Dat wil zeggen dat OMO het doel niet op een andere manier kan bereiken. Zijn er bijvoorbeeld geen andere mogelijkheden, die minder ingrijpend zijn voor de privacy van betrokkenen. Ook mag het cameratoezicht niet op zichzelf staan, geen doel op zich. Het moet onderdeel zijn van een totaalpakket aan maatregelen in het kader van het onderwijs of de beveiliging en sociale veiligheid.

3. Doel en doelbinding

Het inzetten van cameratoezicht, en het gebruik van de (opgenomen) beelden, is alleen toegestaan voor een beperkt aantal vooraf vastgestelde doelen. Voor het onderwijs zijn dit:

1. De continuïteit van (goed) onderwijs op afstand voor leerlingen die vanwege gezondheid of overheidsmaatregelen niet in staat zijn onderwijs fysiek te volgen;
2. de bescherming van de veiligheid en gezondheid van leerlingen, medewerkers en bezoekers;
3. de beveiliging van de toegang tot gebouwen en terreinen;
4. de bewaking van zaken die zich in gebouwen of op terreinen bevinden;
5. het vastleggen van incidenten.

4. Privacytoets

OMO voert eerst een privacytoets (DPIA) uit alvorens er besloten wordt tot het inrichten en gebruiken van cameratoezicht. Bij deze toets zijn de instellingsjurist en de functionaris voor gegevensbescherming (FG) betrokken. Bij deze toets wordt de afweging gemaakt tussen de privacybelangen van de leerlingen, medewerkers en bezoekers en de wens om cameratoezicht te gebruiken. Daarbij kan meewegen of camerabeelden alleen 'live' worden meegekeken, of dat er ook beelden worden opgenomen (wat doorgaans als een grotere inbreuk op de privacy wordt gezien). Ook de gebruikte cameratechniek kan relevant zijn: de ene camera- of softwaretechniek kan ingrijpender zijn dan de andere. Ook het maken van opnames met of zonder geluid is belangrijk. Het toepassen van cameratoezicht moet belangrijker zijn dan de mogelijke inbreuk op de privacy van de betrokkenen.

5. Informatieplicht Cameratoezicht

OMO zorgt ervoor dat de leerlingen, medewerkers en bezoekers weten dat er een camera hangt. Bijvoorbeeld door bordjes (bij de ingang) op te hangen, het Reglement Cameratoezicht publiek beschikbaar te stellen en op bijvoorbeeld de website of in de studiegids beknopt uit te leggen dat er gebruik wordt gemaakt van Cameratoezicht.

6. Bewaartermijn Camerabeelden

De camerabeelden worden niet langer bewaard dan noodzakelijk. De Europese Privacytoezichthouder (EDPB) heeft daarvoor een termijn gesteld van maximaal 4 weken. Voor een Incident (diefstal, fraude of mishandeling, etc.) mag de school de

beelden die het Incident betreffen bewaren tot het incident is afgehandeld, waarna die beelden alsnog moeten worden vernietigd.

7. Heimelijk Cameratoezicht

Het gebruik van verborgen camera's zonder daarover de betrokken personen te informeren, is normaal gesproken niet toegestaan. Alleen in geval van duidelijke en concrete vermoedens van bijvoorbeeld diefstal of fraude door leerlingen of medewerkers, mag er onder strikte voorwaarden gebruik worden gemaakt van heimelijk Cameratoezicht. Belangrijk is dat in het Reglement Cameratoezicht is opgenomen dat de leerlingen, medewerkers en bezoekers er vooraf op worden gewezen dat inzet van verborgen camera's in bepaalde situaties (bijvoorbeeld diefstal of fraude) mogelijk is. Voor het toepassen van heimelijk Cameratoezicht gelden aparte regels zoals een extra privacytoets. OMO maakt – bij voorkeur – geen gebruik van heimelijk Cameratoezicht.

8. Beveiliging

De toegang tot en gebruik van camera's en opgenomen Camerabeelden moet adequaat beveiligd zijn. Denk hierbij aan het instellen van de juiste autorisaties: niet iedereen hoeft of mag toegang (te) hebben tot alle beelden. Ook de apparatuur waarop de beelden worden opgenomen of opgeslagen, moet zijn beveiligd door bijvoorbeeld de recorders in een afgesloten kast te plaatsen.

9. Rechten betrokkenen

De privacywet (AVG) geeft leerlingen, medewerkers en bezoekers een aantal rechten. Belangrijk is dat de leerlingen, medewerkers en bezoekers het recht hebben op de beelden in te zien waarop zij zelf te zien zijn. Dit gaat dus niet om beelden waarop enkel hun eigendommen te zien zijn. Een dergelijk inzageverzoek mag worden afgewezen wanneer het inzageverzoek ongespecificeerd is, of als het inzagerecht kennelijk misbruikt wordt. Hiernaast mag een inzageverzoek worden geweigerd in het belang van de voorkoming, opsporing en vervolging van strafbare feiten.

10. Inzage door en verstrekking aan derden

De (opgenomen) Camerabeelden worden alleen intern gebruikt indien dat past binnen de vastgestelde doeleinden voor Cameratoezicht. Derden krijgen alleen inzage in de Camerabeelden met uitdrukkelijke toestemming van de betrokkene. Een andere grond is als inzage of verstrekking van de beelden noodzakelijk is op grond van een wettelijke verplichting of voor de goede vervulling van de (publiekrechtelijke) taak van politie en justitie in het geval van Incidenten en opsporing. Hieronder valt ook het verstrekken van beelden aan bij wet ingestelde inlichtingendiensten zoals de AIVD.

**BIJLAGE B. Aanwijzing plaatsvervangend Beheerder, Technisch beheerder,
Technisch medewerkers**

*De directeur van het OMO-Bureau wijst in het kader van het 'Reglement
Cameratoezicht OMO 2025' de volgende personen aan:*

Plaatsvervangend beheerder	De door de directeur van het OMO-Bureau aangewezen plaatsvervanger
Technisch beheerder	Teamleider IT
Technisch medewerkers	medewerkers dienst IT

BIJLAGE C. Overzicht camera's t.b.v. Cameratoezicht



Beoordeling
cameratoezicht vesti