# REGLEMENT CAMERATOEZICHT
# in relatie tot beveiliging en sociale veiligheid

## Oktober 2023

Datum voorgenomen besluit BMT: d.d. 08-11-2022

Datum instemming OR: d.d. 15-05-2023

Datum definitieve vaststelling BMT: d.d. 02-10-2023

Versie 02-10-2023

# Voorwoord

Cameratoezicht, ook wel bekend onder het Engelse begrip CCTV, wordt in verschillende situaties gebruikt, bijvoorbeeld om personen en eigendommen te beschermen. Gemeentes gebruiken bijvoorbeeld cameratoezicht 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 past in een groter pakket aan fysieke maatregelen dat wordt toegepast om de veiligheid van medewerkers, studenten en bezoekers binnen en in de directe omgeving van locaties van mbo-scholen te waarborgen.

Cameratoezicht mag geen doel op zichzelf zijn. Cameratoezicht maakt deel uit van een totaalpakket aan maatregelen rondom beveiliging en sociale veiligheid binnen een mbo-school.  Op mbo-scholen hangen steeds vaker camera's. Bijvoorbeeld om vernielingen of diefstal tegen te gaan. Maar er is ook sprake van een inbreuk op de privacy van medewerkers, studenten en bezoekers als cameratoezicht wordt toegepast. Daarom mogen mbo-scholen alleen camera's ophangen als zij aan een aantal voorwaarden voldoen. Ook moeten zij ervoor zorgen dat de inbreuk op de privacy zo klein mogelijk is. Het uitgangspunt blijft dat mensen onbevangen zichzelf moeten kunnen zijn. Bijvoorbeeld een camera in kleedruimtes gaat daarom te ver, omdat mensen dan ontkleed in beeld kunnen komen.

Het reglement cameratoezicht heeft betrekking op die locaties van Scalda waar toezicht door middel van camerasystemen wordt ingezet. Het geeft een beschrijving van taken, verantwoordelijkheden en procedures met betrekking tot het cameratoezicht, met het oog op integer gebruik van het camerasysteem en de bescherming van privacy van studenten, medewerkers en bezoekers.

Hoofdstuk 1 beschrijft de randvoorwaarden waaraan cameratoezicht dient te voldoen. Hoofdstuk 2 beschrijft het reglement zoals we het binnen Scalda hebben geregeld.

# 1. Randvoorwaarden cameratoezicht

## *1.1 Verantwoordelijkheid*

Het zorgvuldig omgaan met gegevens is (wettelijk) de verantwoordelijkheid van de school zelf. De AVG wijst het bevoegd gezag, concreet het college van bestuur, aan als verantwoordelijke om de privacy van medewerkers, studenten en bezoekers te regelen. Een school kan deze verantwoordelijkheid niet afwentelen op bijvoorbeeld haar leveranciers (die in het kader van de privacywetgeving ook wel verwerkers worden genoemd). De persoon op wie de persoonsgegevens betrekking hebben, noemen we betrokkene: dat kan een student zijn, maar ook medewerker (docenten, administratief personeel) of zelfs bezoekers.

Wanneer een school een extern beveiligingsbedrijf inhuurt, dan is dat bedrijf een verwerker. Dat betekent onder meer dat de school aparte afspraken (verwerkersovereenkomst) maakt over de toegang tot en gebruik van het camerasysteem en de camerabeelden. Het beveiligingsbedrijf moet zich houden aan de instructies van de school, en dus ook aan het reglement cameratoezicht van de instelling.

Als de school cameratoezicht inzet, dan ligt de eindverantwoordelijkheid daarvoor bij het college van bestuur. Die stelt, met instemming van de ondernemingsraad, een reglement vast met randvoorwaarden en waarborgen waar het toezicht aan moet voldoen. Het college van bestuur kan een deel van haar beslissingsbevoegdheid overdragen aan één of meerdere personen in de organisatie om praktisch uitvoering te geven aan het cameratoezicht. Deze persoon legt verantwoording af aan het college van bestuur.

## *1.2 Randvoorwaarden*

De wetgever geeft een school 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 de Beleidsregels cameratoezicht van 28 januari 2016[1].

## *1.3 Gerechtvaardigd belang*

De school moet een zogeheten gerechtvaardigd belang hebben voor het cameratoezicht. Bijvoorbeeld diefstal tegengaan of de sociale en fysieke veiligheid van studenten, medewerkers en bezoekers beschermen. Hiervoor moet nog een verdiepende LIA (Legitimate Interests Assessment) plaatsvinden.

Bij een LIA worden 3 punten beoordeeld:

- Beoordeel of er een gerechtvaardigd belang aan is.

[1] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_cameratoezicht-.pdf

- Beoordeel of de verwerking noodzakelijk is voor het doel dat u wilt bereiken.
- Beoordeel de impact op de belangen en rechten en vrijheden van de betrokkenen.

Deze beoordeling worden vastgelegd in het DPIA archief.

## *1.4 Noodzaak cameratoezicht*

Het cameratoezicht moet noodzakelijk zijn. Dat wil zeggen dat de school het doel niet op een andere manier kan bereiken. De school moet eerst nagaan of er geen andere mogelijkheid, die minder ingrijpend is voor de privacy van betrokkenen. Ook mag het cameratoezicht niet op zichzelf staan. Het moet onderdeel zijn van een totaalpakket aan maatregelen in het kader van beveiliging en sociale veiligheid.

## *1.5 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:

a. de bescherming van de veiligheid en gezondheid van studenten, medewerkers en bezoekers;
b. de beveiliging van de toegang tot gebouwen en terreinen;
c. de bewaking van zaken die zich in gebouwen of op terreinen bevinden;
d. het vastleggen van incidenten.

Het gebruik van de camerabeelden voor bijvoorbeeld interne trainingen of educatieve doeleinden, is dus niet toegestaan. Onder deze doelen valt niet het gebruik van camerabeelden voor absentie- of aanwezigheidscontrole of als personeelsvolgsysteem.

## *1.6 DPIA*

De school moet eerst een DPIA uitvoeren alvorens er besloten wordt tot het inrichten en gebruiken van cameratoezicht. Bij deze toets kunnen meerdere functionarissen worden betrokken zoals bijvoorbeeld de instellingsjurist, privacy officer of functionaris voor gegevensbescherming. Bij deze toets maakt de school de afweging tussen de privacybelangen van de studenten, medewerkers en bezoekers en de wens van de school om cameratoezicht te gebruiken. Daarbij kan meewegen of camerabeelden alleen ‘live’ worden meegekeken, of dat er ook beelden worden opgenomen. Dit laatste wordt doorgaans als een grotere inbreuk op de privacy 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. De mbo-school moet kunnen uitleggen waarom het toepassen van cameratoezicht belangrijker is dan de mogelijke inbreuk op de privacy van de betrokkenen. In het kader van de transparantie en verantwoordingsplicht van het college van bestuur, is het raadzaam om de uitkomsten van de DPIA schriftelijk vast te leggen.

## *1.7 Informatieplicht cameratoezicht*

De mbo-school moet ervoor zorgen dat de studenten, 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.

## *1.8 Bewaartermijn camerabeelden*

De school mag de camerabeelden niet langer bewaren dan noodzakelijk is. De richtlijn van de Autoriteit Persoonsgegevens is gesteld op maximaal 4 weken. Voor een geconstateerd incident (diefstal, fraude of mishandeling, etc.) mag de school de incident betreffende beelden bewaren tot het incident is afgehandeld, waarna die beelden moeten worden vernietigd.

## *1.9 Heimelijk cameratoezicht*

Het gebruik van verborgen camera's, zonder daarover de betrokken personen te informeren, is normaal gesproken niet toegestaan. Alleen in geval de school duidelijke en concrete vermoedens van bijvoorbeeld diefstal of fraude door studenten of medewerkers heeft, mag er onder strikte voorwaarden gebruik worden gemaakt van heimelijk cameratoezicht. Belangrijk is dat in het reglement cameratoezicht de studenten, medewerkers en bezoekers vooraf er op gewezen zijn dat verborgen camera's in bepaalde situaties (bijvoorbeeld diefstal of fraude) mogelijk zijn. Het heimelijk cameratoezicht moet zelf ook beperkt zijn: bij overlast in de avonduren is het overdag toepassen daarvan niet proportioneel; evenmin is het filmen van een gehele gang niet noodzakelijk indien er zich alleen bij één specifieke deur incidenten voordoen.

## *1.10 Meldingsplicht cameratoezicht*

Het toepassen van cameratoezicht hoeft in beginsel niet te worden gemeld bij de Autoriteit Persoonsgegevens (of functionaris voor gegevensbescherming indien deze binnen de mbo-school is aangesteld). Er moet dan wel voldaan zijn aan de hiervoor genoemde randvoorwaarden, en het gaat om duidelijk zichtbare camera's.
Bij heimelijk cameratoezicht is een DPIA[2] verplicht.

## *1.11 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 toegang te hebben tot alle beelden. Ook de apparatuur waarop de

[2] https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia

beelden worden opgenomen of opgeslagen, moeten zijn beveiligd door bijvoorbeeld de recorders in een afgesloten kast of ruimte te plaatsen. Houd ook rekening met technisch of functioneel beheer, en het verkrijgen van fysieke toegang tot de opgenomen beelden (toegang serverruimte bijvoorbeeld).

## *1.12 Rechten betrokkenen*

De wet geeft studenten, medewerkers en bezoekers een aantal rechten. Belangrijk is om te beseffen dat de studenten, 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. Dit verzoek mag niet worden geweigerd om personele of administratieve lasten van de mbo-school te beperken. Wél mag een dergelijk inzageverzoek worden afgewezen wanneer het inzageverzoek ongespecificeerd is, of als het inzagerecht kennelijk misbruikt wordt, of wanneer de privacy van anderen in het geding is[3]. Hiernaast mag een inzageverzoek worden geweigerd als het noodzakelijk is in het belang van de voorkoming, opsporing en vervolging van strafbare feiten.

## *1.13 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.

## *1.14 Rol van de ondernemingsraad*

Cameratoezicht betreft de privacy van studenten, medewerkers en bezoekers. Bij het vaststellen, wijzigen of intrekken van het reglement cameratoezicht, wordt de ondernemingsraad op grond van artikel 27 lid 1 onder K WOR om instemming gevraagd. Het gaat immers om ‘een regeling omtrent het verwerken van alsmede de bescherming van de persoonsgegevens van de in de onderneming werkzame personen’. Voor wat betreft studenten is er geen expliciet recht op instemming met het reglement cameratoezicht. De mogelijkheid bestaat dat de studentenraad met dat reglement moet instemmen volgens artikel 8a.2.2 lid 3 onder k WEB: besluiten van het college van bestuur over de regels op het gebied van veiligheid, gezondheid en welzijn.

[3] Zie de richtlijn van de Autoriteit Persoonsgegevens voor een toelichting.

# 2. Reglement cameratoezicht

Dit reglement cameratoezicht heeft betrekking op alle locaties van Scalda waar toezicht door middel van camerasystemen wordt ingezet. Het geeft een beschrijving van taken, verantwoordelijkheden en procedures over het cameratoezicht, met het oog op integer gebruik van het camerasysteem en de bescherming van privacy van studenten, medewerkers en bezoekers.

Cameratoezicht wordt binnen Scalda ingezet tegen wangedrag, diefstal en beschadiging van eigendommen. Daarvoor zijn er voldoende camera's geplaatst bij de ingangen, verkeersruimtes, in de buurt van lockers en fietsenstallingen.
Scalda stelt dat het bedrijfsbelang zwaarder weegt dan het privacybelang van de studenten en medewerkers en zet daarom camera's in. Wel wordt middels dit reglement geborgd dat de privacy niet geschonden wordt.
Bij de ingang van alle Scalda panden is duidelijk zichtbaar aangegeven dat er cameratoezicht is. Zo weten studenten en medewerkers dat zij gefilmd worden.

Het cameratoezicht bij Scalda draagt bij aan:

a. het bevorderen van het veiligheidsgevoel van studenten, medewerkers en derden die verblijven en/of werken in de Scalda gebouwen en –terreinen;
b. het verminderen van schade;
c. het weren van overlast;
d. het voorkomen van vandalisme;
e. het voorkomen van criminele activiteiten;
f. het beveiligen van eigendommen.

Subdoel in relatie tot d, e en f is het bevorderen van de opsporing en vervolging van strafbare feiten.

**Noot:** Camera's geplaatst binnen een examen- en/of lesomgeving en die een ander doel dienen dan hierboven beschreven vallen buiten de scope. Deze camera's worden niet opgenomen binnen het camerasysteem.

## Artikel 1 - Begripsbepalingen

a. *Cameratoezicht*
   toezicht met behulp van camera's, waardoor er sprake is van verwerking van persoonsgegevens als bedoeld in de Wet bescherming persoonsgegevens.
b. *Heimelijk cameratoezicht*
   toezicht met behulp van verborgen en/of niet-zichtbare camera's, of cameratoezicht dat niet kenbaar is gemaakt aan studenten, medewerkers en bezoekers.
c. *Serverruimte*
   de van een toegangscontrolesysteem voorziene ruimte, waar de server of opnameapparatuur staat waarop de opgenomen camerabeelden geregistreerd staan.
d. *Camerasysteem*
   het geheel van camera's, monitoren, opnameapparatuur, verbindingskasten en verbindingen waarmee het cameratoezicht wordt uitgevoerd.
e. *Camera observatieruimte (conciërge loge)*
   een centraal gesitueerde, van een toegangscontrolesysteem voorziene ruimte, waarin de camerabeelden centraal live worden bekeken en/of waar ook de mogelijkheid bestaat om opgenomen camerabeelden terug te kijken en/of op een informatiedrager te plaatsen.
f. *Camerabeeld of beeldinformatie*
   de door het cameratoezicht verkregen camerabeeld.
g. *Beheerder*
   de door het college van bestuur aangewezen medewerker van de school die verantwoordelijk is voor de inrichting, het beheer en toezicht op het cameratoezicht. Deze zorgt voor de continuïteit van het cameratoezicht. Deze kan medewerkers autoriseren tot het bekijken van beelden.
h. *Technisch beheer*
   de zorg voor het technisch functioneren van het camerasysteem.
i. *Technisch beheerder*
   de functionaris, die onder verantwoordelijkheid van de beheerder, is belast met het technisch beheer van het camerasysteem.
j. *Locatiebeheerder / operationeel beheerder*
   een door de beheerder als zodanig aangewezen persoon die belast is met het cameratoezicht op één of meerdere locaties van de school. Deze persoon kan op locatie dat deel van het camerasysteem bedienen waarvoor hij is geautoriseerd.
k. *Bevoegde medewerker / geautoriseerd Scalda medewerker*
   een door de (locatie)beheerder als zodanig aangewezen persoon die betrokken is bij de uitvoering van het cameratoezicht. Deze persoon is door de locatiebeheerder geautoriseerd tot het bekijken van digitale beelden.
l. *Incident*
   een waargenomen ongewenst en/of strafbaar feit, ongeval of andere gebeurtenis die vraagt om handhaving, onderzoek en/of strafrechtelijke vervolging.
m. *Verwerker*

het bedrijf of organisatie die door de school wordt ingehuurd om een deel van het cameratoezicht te verzorgen.

n. *College van Bestuur*
Bevoegd gezag van Scalda.

o. *Houder*
houder van het camerasysteem: stichting Scalda.

## Artikel 2 – Werkingssfeer en doelstellingen cameratoezicht

a.. Dit reglement is van toepassing op studenten, medewerkers en bezoekers die zich bevinden in de gebouwen of op de terreinen van Scalda.

b. Het inzetten van cameratoezicht, en het gebruik van de camerabeelden, is alleen toegestaan voor:

b.1 De bescherming van de veiligheid en gezondheid van studenten, medewerkers en bezoekers;

b.2 De beveiliging van de toegang tot gebouwen en terreinen, waaronder mede is begrepen het weren van onbevoegde of onbevoegd verklaarde personen;

b.3 De bewaking van zaken die zich in gebouwen of op terreinen bevinden;

b.4 Het vastleggen van incidenten.

c.. Camerabeelden worden uitsluitend gebruikt ten behoeve van de doelstelling zoals genoemd in hoofdstuk 2.

## Artikel 3 – Taken en verantwoordelijkheden

a. Het installeren en beheren van camerabewaking geschiedt onder verantwoordelijkheid van de stichting Scalda, de houder van het camerasysteem. Het behelst het installeren en beheren van cameratoezicht.

b. Alvorens te besluiten tot het instellen of intensiveren van cameratoezicht, voert het College van Bestuur een DPIA uit, waarbij de mate van inbreuk op de privacy van de studenten, medewerkers en bezoekers wordt afgewogen tegen het belang van de school om cameratoezicht te gebruiken. Hierbij wordt meegewogen of de doelstellingen als geformuleerd in artikel 2 tweede lid, op een andere wijze kunnen worden bereikt, met een minder ingrijpend middel dan cameratoezicht.

c. Het hoofd huisvesting is verantwoordelijk voor de plaatsing van camera's en beoordeelt nieuwe aanvragen tot plaatsing.

d. Het technisch beheer van het cameratoezicht geschiedt door de dienst HR&O, afdeling Huisvesting.

e. De technische beheerder ondersteunt en adviseert en voert hierin de regie.

f. De operationeel beheerder van het camerasysteem is werkzaam binnen de lokale facilitaire dienst. Dit zijn het hoofd lokale dienst en/of conciërge.

g. Toegang wordt verleend op drie niveaus;

(A) Het bekijken van live beelden van specifieke camera (´s).
(A)+(B) Het terugkijken van beelden op tape.
(A)+(B)+(C) Het kopiëren van beelden naar een externe informatiedrager ten behoeve van nader onderzoek.

h. In geval van een incident wordt dit bij het hoofd lokale dienst dan wel de geautoriseerde Scalda medewerker gemeld voor het ondernemen van benodigde actie. Van ieder incident maken zij een rapport op. Indien de situatie dit vereist meldt de medewerker dit incident bij zijn leidinggevende, politie, spoedeisende medische hulpverlening (ambulance) of andere hulpverlenende instanties.

## Artikel 4 – Inrichten camerasysteem en beveiliging

a. De technisch beheerder is verantwoordelijk voor de inrichting van het camerasysteem en de plaatsing van de camera's, binnen de kaders van de door het College van Bestuur uitgevoerde DPIA als bedoeld in artikel 3 lid 2.
b. De technisch beheerder zorgt voor 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 camera observatieruimte.
c. Het terugkijken van opgenomen camerabeelden geschiedt in aanwezigheid van ten minste twee daartoe bevoegd verklaarde personen.
d. De met cameratoezicht belaste medewerkers gaan vertrouwelijk en integer om met de kennis die zij tot zich nemen vanwege het cameratoezicht, in het bijzonder met betrekking tot de privacy van studenten, medewerkers en bezoekers. Voor zover daar arbeidsrechtelijk niet in is voorzien, sluit de beheerder daartoe een geheimhoudingsverklaring (conform het model van de instelling) met de locatiebeheerder(s), technisch beheerder en/of bevoegde medewerker(s).
e. De locatie beheerder draagt er zorg voor dat het cameratoezicht kenbaar wordt gemaakt aan studenten, medewerkers en bezoekers op zichtbare en herkenbare wijze, zoals, maar niet beperkt tot, borden en stickers bij de ingang van de gebouwen of terreinen van de school.
f. Voor zover er in het camerasysteem camerabeelden worden opgeslagen, worden deze beelden conform de externe richtlijnen opgeslagen (4 weken). 28 kalenderdagen na de opname worden de beelden automatisch gewist, tenzij er een incident is geconstateerd op basis waarvan het noodzakelijk is de met het incident samenhangende camerabeelden te bewaren. Na afhandeling van het incident worden de betreffende camerabeelden (en eventueel gemaakte kopieën of afdrukken) gewist.
g. Het camerasysteem is zodanig uitgerust dat het terugkijken van opgenomen camerabeelden of het uitgeven daarvan slechts mogelijk is in de camera observatieruimte.

h. Voor zover er live camerabeelden worden uitgekeken in een andere ruimte dan de serverruimte of camera observatieruimte, zijn er technische en organisatorische maatregelen genomen die het onbevoegd meekijken zoveel als redelijkerwijs mogelijk voorkomen.
i. Bevoegd tot het bekijken van live beelden zijn:
    a. De technisch beheerder
    b. De locatie beheerder / operationeel beheerder
    c. De bevoegd medewerker
j. Bevoegd tot het terugkijken van beelden
    a. De technisch beheerder
    b. De locatie beheerder / operationeel beheerder
    c. De bevoegd medewerker mits deze door de technisch beheerder en/of locatie beheerder geautoriseerd is. Onder verantwoordelijkheid van de beheerder of locatiebeheerder en onder nader te stellen voorwaarden en voor een vooraf bepaald doel c.q. een vooraf bepaalde periode mag deze camerabeelden terug te kijken.
k. Bevoegd tot het kopiëren van vastgelegde beelden zijn:
    a. De technisch beheerder
    b. De locatie beheerder / operationeel beheerder
l. Voor zover er bij het inrichten van het camerasysteem voor gekozen wordt om de studenten, medewerkers en bezoekers via een monitor live terugkoppeling te geven van de camerabeelden, kunnen deze live camerabeelden alleen betrekking hebben op deze betreffende studenten, medewerkers en bezoekers.
m. Bewerking van camerabeelden vindt slechts plaats in het kader van het verscherpen van deze camerabeelden.

## Artikel 5 – Inzage en uitgifte opgenomen camerabeelden aan derden

a. 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 diens publiekrechtelijke taak.
b. 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.
c. Alvorens tot inzage of uitgifte over te gaan, legitimeert de betreffende functionaris zich vooraf ten overstaan van de beheerder of locatiebeheerder, en tekent voor ontvangst van de uitgegeven camerabeelden.
d. De inzage en uitgifte wordt door de beheerder of locatiebeheerder geregistreerd.
e. Aan andere derden wordt geen inzage in de camerabeelden gegeven, of camerabeelden uitgegevens, anders dan met de uitdrukkelijke toestemming van de betrokken student, medewerker of bezoekers.

## Artikel 6 – Rechten van betrokkenen

a. Betrokken studenten, medewerkers en bezoekers komen de rechten toe zoals bedoeld in de Wet bescherming persoonsgegevens. Hieronder vallen het recht op inzage, correctie en verwijdering van camerabeelden waarop zij zijn afgebeeld.
b. Een verzoek tot inzage in camerabeelden geschiedt schriftelijk of per e-mail aan de beheerder, die binnen 10 werkdagen na ontvangst van het verzoek inhoudelijk zal reageren.
c. Het verzoek tot inzage wordt afgewezen wanneer het verzoek tot inzage in camerabeelden ongespecificeerd is, de identiteit van de verzoeker niet vastgesteld kan worden, of als met dit verzoek kennelijk misbruikt van recht wordt gemaakt.
d. 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.
e. Voor klachten over de toepassing van het camerasysteem, dit reglement en over het gedrag van de beheerder, locatiebeheerder of de bevoegde medewerkers, worden de reguliere klachtenprocedure gevolgd zoals die door het College van Bestuur is vastgesteld

## Artikel 7– Heimelijk cameratoezicht

a. Heimelijk cameratoezicht is slechts toegestaan indien regulier cameratoezicht en andere door de school genomen maatregelen en inspanningen, niet hebben geleid tot beëindiging van de structurele incidenten. Het inzetten van heimelijk cameratoezicht is niet mogelijk voor preventieve doeleinden.
b. Voornoemd heimelijk cameratoezicht mag alleen tijdelijk en op zodanige wijze worden ingezet, dat sprake is van een minimale inbreuk op de persoonlijke levenssfeer van de studenten, medewerkers en bezoekers.
c. Heimelijk cameratoezicht is uitsluitend toegestaan na specifieke voorafgaande schriftelijke toestemming van het College van Bestuur en onder vermelding van de voorwaarden waaronder het heimelijk cameratoezicht plaatsvindt.
d. De school informeert, voor zover redelijkerwijs mogelijk, achteraf betrokken studenten, medewerkers en bezoekers over het toegepaste heimelijk cameratoezicht.
e. Voordat heimelijk cameratoezicht wordt toegepast, voert het College van Bestuur een DPIA uit

## Artikel 8 – Verslaglegging ,en  rapportage en evaluatie

a. De beheerder rapporteert tenminste jaarlijks aan het College van Bestuur over het toegepaste cameratoezicht, waaronder begrepen is een verslag over de verstrekkingen van camerabeelden zoals bedoeld in artikel 5.
b. Jaarlijks wordt door het College van Bestuur gerapporteerd aan de Ondernemingsraad over het cameratoezicht betreffende het voorafgaande jaar (over aard, frequentie en lengte van het toezicht). Daarbij wordt specifiek gemeld indien heimelijk cameratoezicht is toegepast.
c. Op basis van de rapportage vindt een evaluatie plaats en kan dit reglement (deels) herzien worden.

## Artikel 9 – Slotbepalingen

a. Het BMT telt dit reglement vast. Voorafgaand aan het vaststellen, wijzigen of intrekken van dit reglement cameratoezicht, vraagt het College van Bestuur de ondernemingsraad om instemming.
b. Het College van Bestuur informeert de studentenraad over het vaststellen, wijzigen of intrekken van dit reglement, in het geval dat de studentenraad de bevoegdheid is gegeven om in te stemmen met of te adviseren over dit reglement. Voorafgaand aan het vaststellen, wijzigen of intrekken van dit reglement cameratoezicht, vraagt het College van Bestuur de studentenraad om instemming/advies.
c. Het reglement treedt onmiddellijk in werking. Een wijziging in dit reglement treedt in werking binnen 30 dagen na bekendmaking van de wijziging.

## Artikel 10 Klachten

Op dit reglement is de algemene klachtenregeling van Scalda van toepassing.