REGLEMENT CAMERATOEZICHT

ROC van Amsterdam
ROC van Flevoland
Voortgezet Onderwijs van Amsterdam

Uitgave	: ROC van Amsterdam / ROC van Flevoland
Auteur	: E. Siebers / Stuurgroep FSR
Kenmerk	: Reglement Cameratoezicht DEF
Vastgesteld door de Colleges van Bestuur op	: 30-10-2017
Beschikbaar voor Platform OR ROCvA en OR ROCvF	: 09-01-2018 instemming
Beschikbaar voor CSR ROCvA en ROCvF	: 20-12-2017 instemming
Beschikbaar voor GMR VOvA	: 19-04-2018 instemming

Facilitair Samenwerkingsverband ROC's

Cameratoezicht binnen scholen		
Project / Werkgroep	:	FSR
Auteur(s)	:	Stuurgroep FSR
MBO Raad	:	Houttuinlaan 6 Postbus 2051 3440 DB Woerden T: 0348 - 75 35 00 E: info@MBOraad.nl I: www.MBOraad.nl

Hoewel dit document zorgvuldig is opgesteld, kunnen hieraan geen rechten worden ontleend. Iedere instelling is te allen tijde zelf verantwoordelijk voor een juiste toepassing van relevante wet- en regelgeving bij het gebruik van cameratoezicht.

Inhoudsopgave

1 Inleiding

Cameratoezicht, ook wel bekend onder het Engelse begrip CCTV, wordt in verschillende situaties gebruikt, bijvoorbeeld om personen en eigendommen te beschermen. Gemeenten 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 de diverse locaties te waarborgen. Om de leesbaarheid van dit stuk te bevorderen wordt vanaf dit punt met *de diverse locaties* of *een locatie* gerefereerd aan; de mbo-scholen van stichting ROC van Amsterdam (ROCvA) en stichting ROC van Flevoland (ROCvF), de vo-scholen van stichting Voortgezet Onderwijs van Amsterdam (VOvA) en locaties waar stichting Educatie is gehuisvest.

Cameratoezicht mag geen doel op zichzelf zijn. Cameratoezicht maakt deel uit van een totaalpakket aan maatregelen rondom beveiliging en sociale veiligheid binnen een locatie.

Op de diverse locaties hangen steeds vaker camera's. Bijvoorbeeld om vernielingen of diefstal tegen te gaan. Maar ook is sprake van een inbreuk op de privacy van medewerkers, studenten en bezoekers als cameratoezicht wordt toegepast. Daarom mogen de diverse locaties 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.

Deze handreiking helpt de diverse locaties om het gebruik van camera's goed te regelen en daarbij de privacy van medewerkers, studenten en bezoekers te waarborgen. Het model Reglement Camera-toezicht heeft betrekking op de diverse locaties 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.

1.1 Randvoorwaarden cameratoezicht

Verantwoordelijkheid

Het zorgvuldig omgaan met gegevens is (wettelijk) de verantwoordelijkheid van de diverse locaties zelf. De Wet bescherming persoonsgegevens[1] wijst het bevoegd gezag, concreet de Raad van Bestuur (RvB), 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 *bewerkers* worden genoemd). De persoon op wie de persoonsgegevens betrekking hebben, noemen wij *betrokkene*: dat kan een student zijn maar ook een medewerker (docenten, administratief personeel) of zelfs een bezoeker.

Wanneer een locatie een extern beveiligingsbedrijf inhuurt, dan is dat bedrijf een bewerker. Dat betekent onder meer dat de locatie aparte afspraken (bewerkersovereenkomst) maakt over toegang tot en gebruik van het camerasysteem en de camerabeelden. Het beveiligingsbedrijf moet zich houden aan de instructies van de locatie en dus ook aan het Reglement Cameratoezicht van de instelling.

Als een locatie cameratoezicht wil inzetten, dan ligt de eindverantwoordelijkheid daarvoor bij de RvB. Die stelt, met instemming van de ondernemings- en studentenraad, een reglement vast met randvoorwaarden en waarborgen waar het toezicht aan moet voldoen. De RvB kan een deel van haar beslissingsbevoegdheid overdragen aan één of meerdere personen binnen de organisatie om praktisch uitvoering te geven aan het cameratoezicht. Denk bijvoorbeeld aan een directeur Bedrijfsvoering, Veiligheidscoördinator, hoofd Beveiliging, manager HRM of facilitair manager. Deze persoon legt verantwoording af aan de RvB.

Randvoorwaarden

De wetgever geeft een locatie 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[2].

- **Gerechtvaardigd belang**

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

- **Noodzaak cameratoezicht**

Het cameratoezicht moet noodzakelijk zijn. Dat wil zeggen dat de locatie het doel niet op een andere manier kan bereiken. De locatie moet eerst nagaan of geen andere mogelijkheid bestaat 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] Vanaf 25 mei 2018 is dit de Algemene Verordening Gegevensbescherming

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

- **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:

- de bescherming van de veiligheid en gezondheid van studenten, medewerkers en bezoekers;
- de beveiliging van de toegang tot gebouwen en terreinen;
- de bewaking van zaken die zich in gebouwen of op terreinen bevinden;
- 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.

- **Privacy toets**

De locatie moet eerst een privacy toets uitvoeren alvorens besloten wordt tot het inrichten en gebruiken van cameratoezicht. Betrek bij deze toets de instellingsjurist, privacy officer of functionaris voor gegevensbescherming. Bij deze toets maakt de locatie de afweging tussen de privacybelangen van de studenten, medewerkers en bezoekers en de wens van de locatie om cameratoezicht te gebruiken. Daarbij kan meewegen of camerabeelden alleen 'live' worden meegekeken of dat beelden ook 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. De locatie 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 de RvB is het raadzaam om de uitkomsten van de privacy toets schriftelijk vast te leggen.

- **Informatieplicht cameratoezicht**

De locatie moet ervoor zorgen dat de studenten, medewerkers en bezoekers weten dat daar een camera hangt. Bijvoorbeeld door bordjes (bij de ingang) op te hangen, het Reglement Cameratoezicht publiek beschikbaar te stellen en bijvoorbeeld op de website of in de Studiegids beknopt uit te leggen dat gebruik wordt gemaakt van cameratoezicht.

- **Bewaartermijn camerabeelden**

De locatie mag de camerabeelden niet langer dan noodzakelijk bewaren. 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.

- **Heimelijk cameratoezicht**

Het gebruik van verborgen camera's, zonder daarover de betrokken personen te informeren, is normaal gesproken niet toegestaan. Alleen in geval een locatie duidelijke en concrete vermoedens, van bijvoorbeeld diefstal of fraude door studenten of medewerkers, heeft mag onder strikte voorwaarden gebruik worden gemaakt van heimelijk cameratoezicht. Belangrijk is dat in het Reglement Cameratoezicht de studenten, medewerkers en bezoekers vooraf worden gewezen op de mogelijkheid van verborgen camera's in bepaalde situaties (bijvoorbeeld diefstal of fraude). Het heimelijk cameratoezicht zelf moet 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 zich alleen bij één specifieke deur incidenten voordoen.

- **Meldingsplicht cameratoezicht**

Het toepassen van cameratoezicht hoeft - in beginsel - niet te worden gemeld[3] bij de Autoriteit Persoonsgegevens (of functionaris voor gegevensbescherming indien deze binnen de locatie is aangesteld). Dan moet wel voldaan zijn aan de hiervoor genoemde randvoorwaarden en als het gaat om duidelijk zichtbare camera's. De vrijstelling geldt dus niet voor heimelijk cameratoezicht: dat moet nadrukkelijk wél worden gemeld.

- **Beveiliging**

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

- **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 om de beelden in te zien waarop zij zélf 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 locatie te beperken. Wél mag een dergelijk inzageverzoek worden afgewezen wanneer het inzageverzoek ongespecificeerd is, of als het inzagerecht kennelijk misbruikt wordt[4]. Hiernaast mag een inzageverzoek worden geweigerd als het noodzakelijk is in het belang van de voorkoming, opsporing en vervolging van strafbare feiten.

- **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 (publiek-rechtelijke) 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.

- **Rol van de ondernemingsraad en studentenraad**

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 1sub l, van de WOR om instemming gevraagd. Het gaat immers om 'een regeling omtrent het verwerken van, alsmede de bescherming van, de persoonsgegevens van de binnen de onder-neming werkzame personen'. Voor wat betreft studenten bestaat geen expliciet recht op instemming op het Reglement Cameratoezicht. De mogelijkheid bestaat dat de Studentenraad met dat reglement moet instemmen volgens artikel 8a.2.2 lid 3, van de WEB: besluiten van de RvB over de regels op gebied van veiligheid, gezondheid en welzijn.

[3] Artikel 38 Vrijstellingsbesluit Wbp

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

1.2 Do's en don'ts

Do's

- Zorg bij de ingangen van de gebouwen of ruimten voor duidelijke borden en stickers waarop gemeld is dat cameratoezicht wordt toegepast.
- Zorg dat het Reglement Cameratoezicht door de RvB wordt vastgesteld en dat daarmee wordt ingestemd door de ondernemingsraad en studentenraad.
- Zorg vooraf voor een transparante verdeling van rechten en bevoegdheden voor medewerkers die betrokken zijn bij het cameratoezicht.

Don'ts

- Gebruik het cameratoezicht niet voor het beoordelen van functioneren van medewerkers of studenten.
- Pas geen cameratoezicht toe in kleedruimtes of toiletten.
- Pas heimelijk cameratoezicht niet permanent toe.
- Verstrek niet zomaar camerabeelden aan anderen anders dan politie, justitie en inlichtingendiensten (AIVD).

1.3 Sociale veiligheid

Een sociaal veilige school is een school waar géén plaats is voor (ongewenst) grensoverschrijdend gedrag. Sociale veiligheid is het zich beschermd weten en voelen tegen (dreiging van) gevaar. Dit heeft betrekking op alle groepen in de school; tussen studenten onderling, tussen personeelsleden onderling en tussen personeelsleden en (minderjarige) studenten en / of ouders.

Grensoverschrijdend gedrag kent verschillende uitingsvormen:

- Agressie en geweld.
- Verbaal geweld.
- Seksuele intimidatie.
- Pesten.
- Discriminatie.
- Negeren / sociale uitsluiting.

2 Reglement Cameratoezicht

Dit Reglement Cameratoezicht heeft betrekking op alle locaties binnen ROCvA - ROCvF 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.

Artikel 1 – Begripsbepalingen

1. In dit reglement wordt verstaan onder:

- **a.** Cameratoezicht: toezicht met behulp van camera's, waardoor 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: een centraal gesitueerde, van een toegangscontrolesysteem voorziene ruimte, waar de camerabeelden - van alle ruimten - 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: de door het cameratoezicht verkregen camerabeeld.
- **g.** Beheerder: de door de RvB aangewezen medewerker van de locatie die verantwoordelijk is voor de inrichting, het beheer en toezicht op het cameratoezicht.
- **h.** Locatiebeheerder: een door de beheerder als zodanig aangewezen persoon die belast is met het cameratoezicht op één of meerdere locaties.
- **i.** Technisch beheerder: de functionaris die, onder verantwoordelijkheid van de beheerder, is belast met het technisch beheer van het camerasysteem.
- **j.** Bevoegde medewerker: een door de (locatie)beheerder als zodanig aangewezen persoon die betrokken is bij de uitvoering van het cameratoezicht.
- **k.** Incident: een waargenomen ongewenst en / of strafbaar feit, ongeval of andere gebeurtenis die vraagt om handhaving, onderzoek en / of strafrechtelijke vervolging.
- **l.** Bewerker: het bedrijf of de organisatie die door de locatie wordt ingehuurd om een deel van het cameratoezicht te verzorgen.

Artikel 2 – Werkingssfeer en doelstellingen cameratoezicht

1. Dit reglement is van toepassing op studenten, medewerkers en bezoekers die zich bevinden in de gebouwen of op de terreinen van de koepelstichting ROC van Amsterdam en ROC van Flevoland.

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

- **a.** de bescherming van de veiligheid en gezondheid van studenten, medewerkers en bezoekers;
- **b.** de beveiliging van de toegang tot gebouwen en terreinen, waaronder mede is begrepen het weren van onbevoegde of onbevoegd verklaarde personen;
- **c.** de bewaking van zaken die zich in gebouwen of op terreinen bevinden;
- **d.** het vastleggen van incidenten.

3. Camerabeelden worden uitsluitend gebruikt ten behoeve van de doelstelling zoals genoemd in lid 2.

Artikel 3 – Taken en verantwoordelijkheden

1. Het cameratoezicht geschiedt onder verantwoordelijkheid van de RvB.

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

3. De RvB wijst een beheerder aan die verantwoordelijk is voor de inrichting, het beheer en het toezicht op het cameratoezicht binnen de locatie, alsmede een technisch beheerder die, onder verantwoordelijkheid van de beheerder, belast is met het technisch beheer van het camerasysteem.

4. De beheerder wijst bevoegde medewerkers aan, en zo nodig een of meer locatiebeheerder(s).

5. De beheerder wijst voor zichzelf en voor de locatiebeheerder een plaatsvervanger aan, die in geval van afwezigheid van de beheerder respectievelijk locatiebeheerder in diens taken en verantwoordelijkheden treedt.

6. De beheerder, locatiebeheerder(s) en bevoegde medewerkers zijn bevoegd tot het live uitkijken van camerabeelden.

7. De beheerder en locatiebeheerder zijn bevoegd tot het terugkijken en uitgeven van opgenomen camerabeelden.

8. De beheerder en locatiebeheerder kunnen een bevoegde medewerker autoriseren om - onder verantwoordelijkheid van de beheerder of locatiebeheerder - onder nader te stellen voorwaarden en voor een vooraf bepaald doel c.q. een vooraf bepaalde periode camerabeelden terug te kijken.

9. In geval de RvB een bewerker inschakelt, geeft deze de bewerker de opdracht om te handelen conform dit reglement.

Artikel 4 – Inrichten camerasysteem en beveiliging

1. De beheerder is verantwoordelijk voor de inrichting van het camerasysteem en de plaatsing van de camera's binnen de kaders van de door de RvB uitgevoerde privacy toets als bedoeld in artikel 3, lid 2.
2. De 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.
3. Het terugkijken van opgenomen camerabeelden geschiedt in aanwezigheid van ten minste twee daartoe bevoegd verklaarde personen.
4. 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).
5. De beheerder draagt zorg voor het kenbaar maken van cameratoezicht kenbaar aan studenten, medewerkers en bezoekers op zichtbare en herkenbare wijze, zoals - maar niet beperkt tot - borden en stickers bij de ingang van de gebouwen en / of terreinen van de locatie.
6. Voor zover in het camerasysteem camerabeelden worden opgeslagen worden deze beelden uiterlijk vier weken na de opname automatisch gewist, tenzij 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.
7. Het camerasysteem is zodanig uitgerust dat het terugkijken van opgenomen camerabeelden of het uitgeven daarvan slechts mogelijk is in de camera-observatieruimte.
8. Voor zover live camerabeelden worden uitgekeken in een andere ruimte dan de serverruimte of camera-observatieruimte, zijn technische en organisatorische maatregelen genomen die het onbevoegd meekijken zoveel als redelijkerwijs mogelijk voorkomen.
9. Voor zover bij het inrichten van het camerasysteem ervoor 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.
10. Bewerking van camerabeelden vindt slechts plaats in het kader van het verscherpen van deze camerabeelden.

Artikel 5 – Inzage en uitgifte opgenomen camerabeelden aan derden

1. 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.
2. 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.
3. 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.
4. De inzage en uitgifte wordt door de beheerder of locatiebeheerder geregistreerd.
5. Aan andere derden wordt geen inzage in de camerabeelden gegeven, of camerabeelden uit gegevens, anders dan met de uitdrukkelijke toestemming van de betrokken student, medewerker of bezoeker.

Artikel 6 – Rechten van betrokkenen

1. 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.
2. 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.
3. 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.
4. 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.
5. Voor klachten over de toepassing van het camerasysteem, dit reglement en over het gedrag van de beheerder, locatiebeheerder of de bevoegde medewerkers wordt de reguliere klachtenprocedure gevolgd zoals die door de RvB is vastgesteld

Artikel 7 – Heimelijk cameratoezicht

1. Heimelijk cameratoezicht is slechts toegestaan indien regulier cameratoezicht, en andere door de locatie genomen maatregelen en inspanningen, niet hebben geleid tot beëindiging van de structurele incidenten. Het inzetten van heimelijk cameratoezicht is niet mogelijk voor preventieve doeleinden.
2. 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.
3. Heimelijk cameratoezicht is uitsluitend toegestaan na specifieke voorafgaande schriftelijke toestemming van de RvB en onder vermelding van de voorwaarden waaronder het heimelijk cameratoezicht plaatsvindt.
4. De locatie informeert – voor zover redelijkerwijs mogelijk - achteraf de betrokken studenten, medewerkers en bezoekers over het toegepaste heimelijk cameratoezicht.
5. Voordat heimelijk cameratoezicht wordt toegepast, meldt de RvB haar voornemen bij de Autoriteit Persoonsgegevens. Met heimelijk toezicht wordt niet eerder aangevangen dan na instemming daarmee van de Autoriteit Persoonsgegevens.

Artikel 8 – Verslaglegging en rapportage

1. De beheerder rapporteert tenminste jaarlijks aan de RvB over het toegepaste cameratoezicht, waaronder begrepen een verslag over de verstrekkingen van camerabeelden zoals bedoeld in artikel 5.
2. Jaarlijks wordt door de RvB aan de Ondernemingsraad gerapporteerd over het cameratoezicht betreffende het voorafgaande jaar (over aard, frequentie en lengte van het toezicht). Daarbij wordt specifiek gemeld indien heimelijk cameratoezicht is toegepast.

Artikel 9 – Slotbepalingen

1. De RvB stelt dit reglement vast. Voorafgaand aan het vaststellen, wijzigen of intrekken van dit Reglement Cameratoezicht, vraagt de RvB de Ondernemingsraad om instemming.
2. De RvB 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 Cameratoezicht vraagt de RvB voorafgaand aan het vaststellen, wijzigen of intrekken van dit reglement, vraagt de RvB de Studentenraad om instemming / advies.
3. Het reglement treedt onmiddellijk in werking. Een wijziging in dit reglement treedt in werking binnen 30 dagen na bekendmaking van de wijziging.