

Van	Directeur-Bestuurder Stichting Baasis
Aan	Alle betrokkenen
Datum	1-03-2023
Betreft	Handreiking en Reglement Cameratoezicht Stichting Baasis
Format	YSKN-31007 en YSKN-29112 – 1.0
Bron	Kennisnet

Handreiking en Reglement Cameratoezicht Stichting Baasis


Dit reglement cameratoezicht heeft betrekking op alle locaties van de Stichting Baasis 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 leerlingen, medewerkers en bezoekers.

Auteurs: Monique Odijk (PO) en Ferenc Jacobs (FG)

Versie: 1.1

Datum: 01-03-2023

A large, stylized blue wave graphic that curves across the bottom of the page.

0. Document geschiedenis

0.1. Revisies

Onderstaande tabel beschrijft de geschiedenis van dit document

Versie	Datum	Toelichting
1.0	14-03-2022	Standaard formulier uit YSN naar Baasis opmaak.
1.1	01-03-2023	Kleine aanpassingen.

0.2. Goedkeuring

Dit beleid is goedgekeurd door de onderstaande personen:

Naam	Functie	Versie	Datum
Dhr. F. Kingma	Directeur-Bestuurder Stichting Baasis	1.1	24-03-2023
Dhr. F. Kootstra	Voorzitter GMR Stichting Baasis	1.1	20-03-2023

Inhoud

0. Document geschiedenis	1
0.1. Revisies	1
0.2. Goedkeuring	1
1. Inleiding	3
2. Randvoorwaarden cameratoezicht	4
2.1. Verantwoordelijkheid	4
2.2. Randvoorwaarden	4
2.3. Rol van de GMR	7
2.4. Doen en niet doen	7
3. Reglement cameratoezicht Stichting Baasis	8
Artikel 1 – Begripsbepalingen	8
Artikel 2 – Werkingssfeer en doelstellingen cameratoezicht	9
Artikel 3 – Taken en verantwoordelijkheden	9
Artikel 4 – Inrichten camerasysteem en beveiliging	10
Artikel 5 – Inzage en uitgifte opgenomen camerabeelden aan derden	11
Artikel 6 – Rechten van betrokkenen	11
Artikel 7 – Heimelijk cameratoezicht	11
Artikel 8 – Verslaglegging en rapportage	12
Artikel 9 – Slotbepaling	12

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 o.a. in het kader van veiligheid op straat. Het is hierbij van belang dat organisaties zorgvuldig met camerabeelden omgaan. Stichting Baasis maakt gebruik van cameratoezicht en is van plan dit te gaan doen op meerdere locaties.

Op po- en vo-instellingen hangen steeds vaker camera's. Bijvoorbeeld om vernielingen of diefstal tegen te gaan. Maar hiermee is de inbreuk op de privacy van leerlingen, medewerkers en bezoekers groot. Daarom mogen po- en vo-instellingen 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. Een camera in bijvoorbeeld een toilet gaat te ver, omdat mensen dan ontkleed in beeld kunnen komen.

Het inzetten van cameratoezicht past in een groter pakket aan fysieke maatregelen dat wordt toegepast om de veiligheid van medewerkers, leerlingen en bezoekers binnen en in de directe omgeving van locaties van Stichting Baasis te waarborgen. Cameratoezicht mag geen doel op zichzelf zijn, het maakt deel uit van een totaalpakket aan maatregelen rondom beveiliging en sociale veiligheid bij Stichting Baasis.

Deze 'handreiking cameratoezicht' helpt Stichting Baasis om het gebruik van camera's goed te regelen, en daarbij de privacy van leerlingen, medewerkers en bezoekers te waarborgen. Het bijgesloten 'reglement cameratoezicht' heeft betrekking op die locaties van Stichting Baasis, 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 leerlingen, medewerkers en bezoekers.

2. Randvoorwaarden cameratoezicht

2.1. Verantwoordelijkheid

Het zorgvuldig omgaan met gegevens is (wettelijk) de verantwoordelijkheid van onderwijsinstellingen zelf. De Algemene Verordening Gegevensbescherming (AVG) wijst het bevoegd gezag, concreet de Directeur-Bestuurder, aan als verwerkingsverantwoordelijke om de privacy van leerlingen, medewerkers en bezoekers te regelen. Een instelling kan deze verantwoordelijkheid niet afwentelen op bijvoorbeeld haar leveranciers. Deze worden in het kader van de privacywetgeving in de AVG verwerkers genoemd.

De persoon op wie de persoonsgegevens betrekking hebben, noemen we betrokkene: dat kunnen leerlingen zijn, maar ook medewerkers (docenten, administratief personeel) of zelfs bezoekers. Indien de betrokkene de leeftijd van 16 jaar nog niet bereikt heeft, wordt de betrokkene (de leerling) vertegenwoordigd door zijn wettelijk vertegenwoordiger. Meestal zal dit een ouder zijn, maar een voogd kan ook.

Als een onderwijsinstelling cameratoezicht wil inzetten, dan ligt de eindverantwoordelijkheid daarvoor bij de Directeur-Bestuurder. Die stelt, met instemming van de GMR, een reglement vast met randvoorwaarden en waarborgt waar het toezicht aan moet voldoen. De Directeur-Bestuurder kan een deel van zijn beslissingsbevoegdheid overdragen aan één of meerdere personen in de organisatie om praktisch uitvoering te geven aan het cameratoezicht. Denk bijvoorbeeld aan de bovenschools ICT-coördinator(en) en/of Privacy Officer. Deze leggen verantwoording af aan de Directeur-Bestuurder.

2.2. Randvoorwaarden

De wetgever geeft een onderwijsinstelling 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.

2.2.1. Gerechtvaardigd belang

De onderwijsinstelling moet een zogeheten gerechtvaardigd belang hebben voor het cameratoezicht. Bijvoorbeeld diefstal of vernieling tegengaan; of het beschermen van leerlingen, medewerkers en bezoekers.

2.2.2. 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 leerlingen, 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 ook niet het gebruik van camerabeelden voor absentie- of aanwezigheidscontrole of als personeelsvolgsysteem.

2.2.3. Noodzaak cameratoezicht

Het cameratoezicht moet noodzakelijk zijn. Dat wil zeggen dat de onderwijsinstelling het doel niet op een andere manier kan bereiken. De onderwijsinstelling moet eerst nagaan of er geen andere mogelijkheid is, 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.

2.2.4. Risicoanalyse

De onderwijsinstelling moet eerst een risicoanalyse in de vorm van een 'Data Protection Impact Assessment' (DPIA) uitvoeren alvorens er besloten wordt tot het inrichten en gebruiken van cameratoezicht.

Bij deze analyse weegt de onderwijsinstelling de belangen van de leerlingen, medewerkers en bezoekers af tegen de wens om cameratoezicht te gebruiken. Neem hierin de volgende zaken mee: Worden camerabeelden alleen 'live' meegekeken, of opgenomen (wat doorgaans als een grotere inbreuk op de privacy wordt gezien). De gebruikte camera- of softwaretechniek. Het maken van opnames met of zonder geluid. Betrek hierbij de instellingsjurist, de Privacy Officer, manager informatiebeveiliging en/of de Functionaris voor Gegevensbescherming.

De onderwijsinstelling 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 Directeur-Bestuurder, leggen we de uitkomsten van de risicoanalyse schriftelijk vast in het document: '21001 – DPIA Cameratoezicht (naam school)'.

2.2.5. Informatieplicht cameratoezicht

De onderwijsinstelling moet ervoor zorgen dat de leerlingen en/of hun wettelijk vertegenwoordiger, 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 schoolgids beknopt uit te leggen dat er gebruik wordt gemaakt van cameratoezicht en waarom.

2.2.6. Bewaartermijn camerabeelden

De onderwijsinstelling mag de camerabeelden niet langer bewaren dan noodzakelijk is. De richtlijn van de Autoriteit Persoonsgegevens is hiervoor maximaal 4 weken. Voor een geconstateerd incident, zoals diefstal, fraude of mishandeling, mag de school alleen de betreffende beelden van het incident langer bewaren, namelijk totdat dit incident is afgehandeld.

2.2.7. Heimelijk cameratoezicht

Het gebruik van verborgen camera's, zonder daarover de betrokken personen te informeren, is normaal gesproken niet toegestaan. Alleen in geval een onderwijsinstelling duidelijke en concrete vermoedens van bijvoorbeeld diefstal of fraude door leerlingen of medewerkers heeft, mag er onder strikte voorwaarden gebruik worden gemaakt van heimelijk cameratoezicht. Belangrijk is dat in het reglement cameratoezicht de leerlingen en/of hun wettelijk vertegenwoordiger, medewerkers, en bezoekers vooraf erop 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 avonden 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.

2.2.8. 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 onderwijsinstelling is aangesteld). Er moet dan wel voldaan zijn aan de hiervoor genoemde randvoorwaarden, en het gaat om duidelijk zichtbare camera's. De vrijstelling geldt dus niet voor heimelijk cameratoezicht: dat moet wél worden gemeld.

2.2.9. Beveiliging

De toegang tot en gebruik van camera's en opgenomen camerabeelden moet adequaat beveiligd zijn. Denk hierbij ook 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, moet zijn beveiligd door bijvoorbeeld de recorders in een afgesloten kast te plaatsen. Houd ook rekening met technisch en/of functioneel beheer en het verkrijgen van fysieke toegang tot de opgenomen beelden.

2.2.10. Rechten betrokkenen

De leerlingen en/of hun wettelijk vertegenwoordiger, medewerkers en bezoekers hebben een aantal rechten. Deze worden geregeld in het reglement cameratoezicht. Belangrijk is om te beseffen dat de leerlingen en/of hun wettelijk vertegenwoordiger, medewerkers en bezoekers het recht hebben op inzage in 'hun' camerabeelden. Dit verzoek mag niet worden geweigerd om administratieve lasten van de onderwijsinstelling te beperken. Wél mag een dergelijk inzageverzoek worden afgewezen wanneer het verzoek tot inzage in camerabeelden ongespecificeerd is of als het inzagerecht kennelijk misbruikt wordt. Hiernaast mag een inzageverzoek worden geweigerd als het noodzakelijk is in het belang van de voorkoming, opsporing en vervolging van strafbare feiten.

2.2.11. 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 en/of diens wettelijk vertegenwoordiger. Een andere grond is als inzage of verstrekking van de beelden noodzakelijk is op grond een wettelijke verplichting of voor de goede vervulling van de (publiekrechtelijke) taak van politie en justitie in het geval van incidenten.

2.3. Rol van de GMR

Bij cameratoezicht gaat het over de privacy van leerlingen, medewerkers en bezoekers. Bij het vaststellen, wijzigen of intrekken van het reglement cameratoezicht, wordt de GMR om instemming gevraagd. Het gaat immers om een regeling omtrent het verwerken van alsmede de bescherming van de persoonsgegevens.

2.4. Doen en niet doen

2.4.1 Doen

- Zorg bij de ingangen van de gebouwen of ruimtes voor duidelijke borden en stickers waarop gemeld is dat er cameratoezicht wordt toegepast.
- Zorg dat het reglement cameratoezicht door het de Directeur-Bestuurder wordt vastgesteld en er instemming daarmee is door de GMR.
- Zorg vooraf voor een transparante verdeling van rechten en bevoegdheden voor medewerkers die betrokken zijn bij het cameratoezicht.

2.4.2. Niet doen

- 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 aan politie en justitie.

3. Reglement cameratoezicht Stichting Baasis

Artikel 1 – Begripsbepalingen

1. In dit reglement wordt verstaan onder:
 - a. **Beheerder:** de door de Directeur-Bestuurder aangewezen medewerker van de onderwijsinstelling, die verantwoordelijk is voor de inrichting, het beheer en toezicht op het cameratoezicht (in het algemeen is dit de directeur van de onderwijsinstelling).
 - b. **Bevoegde medewerker:** een door de beheerder [in geval van cameratoezicht op meerdere locaties: de locatiebeheerder] als zodanig aangewezen persoon die betrokken is bij de uitvoering van het cameratoezicht.
 - c. **Bezoeker:** Een ieder die de locatie betreedt en geen medewerker of leerling is, maar wel een duidelijk, gerechtvaardigd doel heeft om op die locatie aanwezig te zijn.
 - d. **Camerabeeld:** de door het cameratoezicht verkregen camerabeeld.
 - e. **Camera-observatieruimte:** een centraal gesitueerde, van een toegangscontrolesysteem voorziene ruimte, waarin de camerabeelden - van alle locaties - 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. **Cameratoezicht:** toezicht met behulp van camera's, waardoor er sprake is van verwerking van persoonsgegevens als bedoeld in de Algemene Verordening Gegevensbescherming (tot 25 mei 2018 Wet bescherming persoonsgegevens).
 - g. **Camerasysteem:** het geheel van camera's, monitoren, opnameapparatuur, verbindingkasten, verbindingen en bevestigingen waarmee het cameratoezicht wordt uitgevoerd.
 - h. **Incident:** een waargenomen ongewenst en/of strafbaar feit, ongeval of andere gebeurtenis die vraagt om handhaving, onderzoek en/of strafrechtelijke vervolging.
 - i. **Heimelijk cameratoezicht:** toezicht met behulp van verborgen en/of niet-zichtbare camera's, of cameratoezicht dat niet kenbaar is gemaakt aan leerlingen en/of hun wettelijk vertegenwoordiger, medewerkers en bezoekers.
 - j. **Locatie:** Een gebouw van Stichting Baasis, dit kan de hoofdlocatie van een school zijn, een dependance, een andere locatie waar onderwijs verzorgd wordt (sporthal/ gymzaal) of het bestuurskantoor.
 - k. **Locatiebeheerder:** een door de beheerder als zodanig aangewezen persoon die belast is met het cameratoezicht op één of meerdere locaties van de onderwijsinstelling.
 - l. **Onderwijsinstelling:** Een school van Stichting Baasis, of het bestuurskantoor zelf.
 - m. **Serverruimte:** de van een toegangscontrolesysteem voorziene ruimte, waar de server of opnameapparatuur staat waarop de opgenomen camerabeelden geregistreerd staan.
 - n. **Technisch beheerder:** de functionaris, die onder verantwoordelijkheid van de beheerder, is belast met het technisch beheer van het camerasysteem.

Artikel 2 – Werkingsfeer en doelstellingen cameratoezicht

1. Dit reglement is van toepassing op leerlingen en/of hun wettelijk vertegenwoordiger, medewerkers en bezoekers die zich bevinden in de gebouwen of op de terreinen van Stichting Baasis.
2. Het inzetten van cameratoezicht, en het gebruik van de camerabeelden, is alleen toegestaan voor:
 - a. de bescherming van de veiligheid en gezondheid van leerlingen, medewerkers en bezoekers;
 - b. de beveiliging van de toegang tot gebouwen en terreinen, waaronder mede is begrepen het weren van ongewenste bezoekers;
 - c. de bewaking van zaken die zich in gebouwen of op terreinen bevinden;
 - d. het vastleggen van incidenten.
3. Camerabeelden worden uitsluitend gebruikt t.b.v. van de doelstelling zoals genoemd in lid 2.

Artikel 3 – Taken en verantwoordelijkheden

1. Het cameratoezicht geschiedt onder verantwoordelijkheid van de Directeur-Bestuurder.
2. Alvorens te besluiten tot het instellen of intensiveren van cameratoezicht, voert de organisatie samen met de Privacy Officer een risicoanalyse (DPIA) uit, waarbij de mate van inbreuk op de privacy van de leerlingen, medewerkers en bezoekers wordt afgewogen tegen het belang van de onderwijsinstelling om cameratoezicht te gebruiken. Hierbij wordt meegewogen of de doelstellingen als geformuleerd in artikel 2, op een andere wijze kunnen worden bereikt, met een minder ingrijpend middel dan cameratoezicht. De uitkomsten worden vervolgens besproken met de MR van de betrokken locatie.
3. De Directeur-Bestuurder wijst een *beheerder* aan die verantwoordelijk is voor de inrichting, het beheer en toezicht op het cameratoezicht op 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 camera- beelden.
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 cq. een vooraf bepaalde periode camerabeelden terug te kijken.

Artikel 4 – Inrichten camerasysteem en beveiliging

1. De beheerder is verantwoordelijk voor de inrichting van het camerasysteem en de plaatsing van de camera's op de locatie, binnen de kaders van de door de Privacy Officer uitgevoerde risicoanalyse (DPIA) 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.
 - a. 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.
 - b. De maatregelen betreffen het camerasysteem, de serverruimte en camera-observatieruimte.
3. Het terugkijken van opgenomen camerabeelden geschiedt slechts in aanwezigheid van twee daartoe bevoegd verklaarde personen.
4. De met cameratoezicht belaste medewerkers gaan vertrouwelijk en integer om met de kennis die zij tot zich krijgen vanwege het cameratoezicht, in het bijzonder met betrekking tot de privacy van leerlingen, medewerkers en bezoekers. Voor zover daar arbeidsrechtelijk niet in is voorzien, sluit de beheerder daartoe een geheimhoudingsverklaring met de locatiebeheerder(s), technisch beheerder en/of bevoegde medewerker(s).
5. De beheerder draagt er zorg voor dat het cameratoezicht kenbaar wordt gemaakt aan leerlingen en/of hun wettelijk vertegenwoordiger, 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 onderwijsinstelling.
6. Voor zover er in het camerasysteem camerabeelden worden opgeslagen, worden deze beelden na uiterlijk 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. Na afhandeling van het incident worden de betreffende camerabeelden (en eventueel gemaakte kopieën of afdrucken) gewist.
7. Het camerasysteem is zodanig uitgerust dat het terugkijken van opgenomen camerabeelden of het uitgeven daarvan slechts mogelijk is in de cameraobservatieruimte.
8. Voor zover er live camerabeelden worden uitgekeken in een andere ruimte dan de serverruimte of cameraobservatieruimte, zijn er technische en organisatorische maatregelen genomen die het onbevoegd meekijken zoveel als redelijkerwijs mogelijk voorkomen.
9. Voor zover er bij het inrichten van het camerasysteem voor 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.
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 uitgegeven, anders dan met de uitdrukkelijke toestemming van de betrokken leerling en/of hun wettelijk vertegenwoordiger, medewerker of bezoeker.

Artikel 6 – Rechten van betrokkenen

1. Betrokken leerlingen en/of hun wettelijk vertegenwoordiger, medewerkers en bezoekers komen de rechten toe zoals bedoeld in de Algemene Verordening Gegevensbescherming (tot 25 mei 2018 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, 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 voorkoming, opsporing en vervolging van strafbare feiten.
5. Klachten over de toepassing van het camerasysteem, dit reglement en over het gedrag van de beheerder, locatiebeheerder of de bevoegde medewerkers, worden schriftelijk ingediend bij de Directeur-Bestuurder. De Directeur-Bestuurder zal binnen 6 weken na datum ontvangst van de klacht reageren.

Artikel 7– Heimelijk cameratoezicht

1. Heimelijk cameratoezicht is slechts toegestaan indien regulier cameratoezicht en andere door de onderwijsinstelling genomen maatregelen en inspanningen, niet leiden 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 inbreuk op de persoonlijke levenssfeer van de leerlingen, medewerkers en bezoekers zo klein mogelijk is.

3. Heimelijk cameratoezicht is uitsluitend toegestaan na specifieke voorafgaande schriftelijke toestemming van de Directeur-Bestuurder onder vermelding van de voorwaarden waaronder het heimelijk cameratoezicht plaatsvindt.
4. De onderwijsinstelling informeert – voor zover redelijkerwijs mogelijk - achteraf de betrokken leerlingen en/of hun wettelijk vertegenwoordiger, medewerkers en bezoekers over het toegepaste heimelijk cameratoezicht.
5. Voordat heimelijk cameratoezicht wordt toegepast, meldt de Directeur-Bestuurder haar voornemen bij de Autoriteit Persoonsgegevens. Er wordt niet eerder aangevangen met heimelijk toezicht dan na instemming daarmee van de Autoriteit Persoonsgegevens.

Artikel 8 – Verslaglegging en rapportage

1. De beheerder rapporteert tenminste jaarlijks aan de Directeur-Bestuurder over het toegepaste cameratoezicht, waaronder begrepen is een verslag over de verstrekkingen van camerabeelden zoals bedoeld in artikel 5.
2. De beheerder rapporteert tenminste jaarlijks aan de directeur van de school over het toegepaste cameratoezicht, specifiek gericht op de locatie(s) waar de directeur verantwoordelijk voor is, waaronder begrepen is een verslag over de verstrekkingen van camerabeelden zoals bedoeld in artikel 5.
3. Jaarlijks wordt door de Directeur-Bestuurder op hoofdlijnen gerapporteerd aan de GMR over het cameratoezicht betreffende het voorafgaande jaar bij Stichting Baasis.
4. Jaarlijks wordt door de directeur van de school gerapporteerd aan de MR 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 – Slotbepaling

1. De Directeur-Bestuurder stelt dit reglement vast.
2. Voorafgaand aan het vaststellen, wijzigen of intrekken van dit reglement cameratoezicht, vraagt de Directeur-Bestuurder de GMR om instemming.
3. Voorafgaand aan het vaststellen, wijzigen of intrekken van een afgenomen DPIA, vraagt de Directeur van de school de MR om instemming.
4. De directeur van de onderwijsinstelling informeert, indien aanwezig, de leerlingenraad over het vaststellen, wijzigen of intrekken van dit reglement.
5. Het reglement treedt onmiddellijk in werking. Een wijziging in dit reglement treedt in werking binnen 30 dagen na bekendmaking van de wijziging.