VEILIGHEIDSBELEIDSPLAN CSG JAN ARENTSZ

2026-2027

VEILIGHEIDSBELEIDSPLAN CSG JAN ARENTSZ 2026-2027

Inleiding

Csg Jan Arentsz wil in de regio herkend worden als een school met een warm en duidelijk schoolklimaat.
Een school met een grote mate van organisatietrots, met medewerkers en leerlingen die zich gewaardeerd voelen. Die zich veilig voelen. Met onderwijs dat een wezenlijke bijdrage levert aan de kwaliteit van het leven van individuen en van de samenleving, dat zich richt op kwalificatie, socialisatie EN persoonsvorming! Met een schoolleiding die zorgt voor duidelijke richtlijnen, die inspireren en ondersteunen daar waar nodig is. Een school ook met een platte organisatie waarin de middelen efficiënt worden aangewend, waardoor bureaucratische omwegen worden voorkomen.

Binnen de CSG Jan Arentsz zijn afspraken gemaakt over de wijze waarop uitvoering wordt gegeven aan deze collectieve ambitie. Vertrouwen is de basis van alle relaties binnen de school en moet zorgen voor een cultuur van 'veilige onzekerheid'. Tegelijkertijd is de ruimte die er is niet onbegrensd. We hebben een aantal gemeenschappelijke afspraken. En in het licht van dit document is ons normatief kader leidend:

Wij hebben respect voor elkaar
Wij nemen onze verantwoordelijkheid
Wij helpen elkaar

INHOUD

Het veiligheidsbeleidsplan kan gezien worden als een kerndocument. Uitwerkingen van de principes die hier beschreven zijn, vinden plaats in hiervan afgeleide documenten.

Inhoudsopgave

1. Algemene opmerkingen 3
2. Gedragscode 5
3. Richtlijnen voor buitenschoolse activiteiten 5
4. Pestprotocol 6
5. Meldcode huiselijk geweld en kindermishandeling 7
6. Meldplicht zedendelicten (MOA Meld Overleg en Aangifteplicht) 8
7. Protocol (seksuele) intimidatie en (seksueel) geweld 8
8. Vertrouwenspersoon (intern en extern) 9
9. Protocol camerabewaking 9
10. Het doen van aangifte op school 10
11. Handelingsprotocol bij ongewenst bezoek op het schoolterrein 11
12. Zorgvuldig omgaan met informatie sociale media 12
13. Procedure melding datalekken 15
14. Informatiebeveiliging en privacy beleid 17
15. Privacyreglement 30
16. Wat als je een zwakke plek vindt in een van onze systemen? 39

Alle documenten zijn te lezen op het intranet onder “veiligheid”

1. Algemene opmerkingen

1. Dit Veiligheidsbeleidsplan geldt voor alle vestigingen van de CSG Jan Arentsz. De afspraken en voorschriften gelden in de gebouwen, op het schoolterrein rond de gebouwen en tijdens alle door de school georganiseerde activiteiten elders.
2. Op het schoolterrein zijn camera's opgehangen ter preventie van crimineel en grensoverschrijdend gedrag.
3. Leerlingen ontvangen een leerlingpas voorzien van naam, klas en foto. De pas dragen zij bij zich als legitimatie. De leerlingpas wordt tevens gebruikt voor het openen van de schoolkluis.
4. De kluisjes binnen school mogen op elk moment geopend worden door daartoe door het bevoegd gezag gemachtigde personen, als er een vermoeden bestaat dat de inhoud daarvan in strijd is met schoolafspraken dan wel met wet- en/of regelgeving. Ook tassen, jassen en andere persoonlijke eigendommen mogen geopend en gecontroleerd worden.
5. Alle incidenten waarbij de rust en de veiligheid van de schoolgemeenschap in het geding is worden gemeld in het incidentenregistratiesysteem van Magister. We maken een onderscheid tussen "incidenten" en "wettelijke incidenten". Een schoolleider of een collega namens deze zal deze registratie verzorgen. Dat laat onverlet dat melding van incidenten door eenieder kan plaatsvinden die hiermee in aanraking komt. Incidenten kunnen ook worden gemaild aan: veiligheid@ja.nl

   Te denken valt hierbij aan (niet uitputtend):
   - Spijbelen
   - (Digitale)Fraude
   - Vandalisme
   - Pesten
   - Discriminatie
   - Bedreigingen
   - Vechtpartijen
   - Mishandeling
   - Wapenbezit waaronder messen
   - Seksuele intimidatie, seksueel geweld
   - Diefstal, heling
   - Gebruik van verslavende middelen of de handel daarin
   - Vuurwerkgebruik in alle categorieën
   - Informatiebeveiliging en privacy

Het gaat hier om incidenten en gedragingen die de rust en de veiligheid verstoren, waarmee de wet wordt overtreden of die niet passen in een cultuur van vertrouwen. We vragen van alle personeelsleden, leerlingen en hun ouders/verzorgers om in deze cultuurdrager te zijn. Het is goed dat we ons steeds afvragen of het grensoverschrijdende gedrag een signaal is voor een dieperliggend probleem. Is dat het geval dat komen zorgteam en externe partijen in beeld die hierbij kunnen helpen.
De schoolleider doet melding in het incidentenregistratiesysteem van alle hierboven genoemde zaken, of draagt er zorg voor dat dit wordt gedaan.

De school is niet verantwoordelijk voor elke vorm van materiële en immateriële schade veroorzaakt door welke vorm van grensoverschrijdend gedrag dan ook. Is er sprake van schade door toedoen van een leerling, dan is de leerling (dan wel zijn ouder(s)/verzorger(s)) aansprakelijk voor de schade. Bij ernstige vormen van grensoverschrijdend gedrag wordt

aangifte gedaan, dan wel wordt leerling en/of de ouders/verzorgers geadviseerd aangifte te doen.

Uiteraard heeft het Jan Arentsz een ontruimingsplan en een BHV team. De ontruimingsplannen zijn bekend bij onze medewerkers. Leerlingen vinden de informatie die zij nodig hebben op de deuren van de klaslokalen en op de ontruimingsplattegronden. Ontruimingen worden regelmatig geoefend.

2. Gedragscode

Ons normatief kader

Wij hebben respect voor elkaar
Wij nemen onze verantwoordelijkheid
Wij helpen elkaar

Vanuit het normatief kader hebben we de gedragscode vastgesteld:

Gedragscode:

- We praten met elkaar en niet over elkaar
- We houden verstoringen zo klein mogelijk
- We ruimen oud zeer zo snel mogelijk op
- We blijven met elkaar in gesprek ook als het moeilijk wordt
- We stellen onze mening uit totdat we volledig zijn geïnformeerd
- We nodigen iedereen die iets heeft bij te dragen uit om mee te praten
- We geven het goede voorbeeld
- We accepteren geen discriminatie in welke vorm dan ook
- We gaan vertrouwelijk om met vertrouwelijke informatie
- We mogen elkaar aanspreken op afspraken en doen dat op een veilige manier

3. Richtlijnen voor buitenschoolse activiteiten

Algemeen
Er is een digitaal formulier opgesteld om buitenschoolse activiteiten zo veilig mogelijk te doen verlopen. Dit formulier dient voorgaande aan een activiteit doorgenomen en ingevuld te worden. Het is terug te vinden op het medewerkersportaal, onder het kopje “Buitenschoolse activiteiten”.

Controlelijst voor buitenschoolse activiteiten

1. **<u>Voorbereiding</u>**

- De bestemming wordt gecheckt op de site van de Rijksoverheid m.b.t. het reisadvies.
- De schoolleider heeft toestemming gegeven ten aanzien van programma, doelgroep, begeleiding, doelstelling, bestemming, begroting en consequenties met betrekking tot de organisatie;
- De schoolleider wordt op de hoogte gehouden van alle relevante reisdetails (zoals begeleiding, vervoer, verblijfplaats, contactmogelijkheden);
- De meldkamer is op de hoogte gebracht van de leerlingen die meegaan, de receptie is op de hoogte gebracht van de activiteit.
- Voor de activiteit wordt een begroting gemaakt (kosten vervoer, kosten entree, kosten consumpties, overige kosten, aantal deelnemende leerlingen, eventueel bijdragen van de school, bedrag per leerling).

2. **Begeleiding**
   - Er is voldoende begeleiding om toezicht te houden.

3. **Calamiteiten**
   - Er gaat een volledige EHBO-doos mee op excursie (bij kamp, werkweek of sport/buitenactiviteit).
   - Het is bekend welke leerlingen medicijnen gebruiken.
   - In geval van wangedrag en wanneer ernstige disciplinaire maatregelen worden overwogen, wordt de schoolleider onmiddellijk geraadpleegd. In overleg wordt bepaald wat er dient te gebeuren.

4. **Ouders/verzorgers en leerlingen**
   - Met de leerlingen is besproken hoe te handelen bij calamiteiten en/of incidenten.
   - Alle essentiële informatie ten aanzien van programma, bereikbaarheid, regels en afspraken is aan de ouders/verzorgers en leerlingen doorgegeven.
   - Alle ouders/verzorgers hebben in het geval van een meerdaagse activiteit schriftelijk toestemming gegeven.

4. Pestprotocol

Voor ons pestprotocol volg deze link. Pestprotocol

5. Meldcode Huiselijk geweld en kindermishandeling

Bij huiselijk geweld en kindermishandeling

De wet Meldcode huiselijk geweld en kindermishandeling verplicht beroepskrachten, ook onderwijspersoneel, om een vijfstappenplan te gebruiken als ze het vermoeden hebben van kindermishandeling en/of huiselijk geweld. Deze wet bestaat al sinds 2013. Het stappenplan dat je moet volgen, bestaat uit deze stappen:

1. In kaart brengen van signalen van huiselijk geweld of kindermishandeling.
2. Collegiale consultatie en zo nodig raadplegen van Veilig Thuis.
3. Gesprek met de ouder(s).

4. Met behulp van een afwegingskader bepalen of er sprake is van acute of structurele onveiligheid. Bij twijfel altijd Veilig Thuis raadplegen.
5. Bij acute of structurele onveiligheid: altijd melden bij Veilig Thuis. Daarnaast is zelf hulp verlenen of organiseren ook mogelijk.

6. Meldplicht zedendelicten (MOA Meld Overleg en Aangifteplicht)

Bij seksueel misbruik in het onderwijs
De Wet bestrijding seksueel misbruik en seksuele intimidatie in het onderwijs wordt ook wel de Meld-, overleg- en aangifteplicht genoemd. Deze wet verplicht alle medewerkers die het vermoeden hebben van, of informatie krijgen over, een mogelijk zedendelict door een medewerker van de school jegens een minderjarige leerling onmiddellijk door te geven aan het bevoegd gezag. Deze wet bestaat al sinds 1999. Het proces dat je moet volgen, bestaat uit deze stappen:

1. Een medewerker van een onderwijsinstelling heeft het vermoeden van, of informatie over, een zedendelict, gepleegd door een medewerker van de school jegens een minderjarige leerling.
2. De medewerker meldt dit aan het bevoegd gezag.
3. Het bevoegd gezag overlegt met de vertrouwensinspecteur.
4. Er is een redelijk vermoeden van een strafbaar feit.
5. Het bevoegd gezag informeert (ouders van) klager en aangeklaagde dat aangifte wordt gedaan.
6. Het bevoegd gezag doet aangifte Lees hier meer over in het artikel Aangifte doen in het Onderwijs. bij justitie of politie.

Https://www.schoolenveiligheid.nl/wp-content/uploads/2023/02/Meldcodemeldplicht-vo-mbo.pdf

7. Protocol (seksuele) intimidatie en (seksueel) geweld

- Het slachtoffer doet melding aan vertrouwenspersoon, docent of ander personeelslid van de school;
- De ontvanger van de melding luistert naar het slachtoffer. Stelt geen vragen. Maakt eventueel na het gesprek aantekeningen van wat gezegd is door het slachtoffer. (de ontvanger van de melding kan later als getuige gehoord worden);
- De ontvanger van de melding schakelt de vertrouwenspersoon van de school in en informeert de veiligheidscoördinator;
- De vertrouwenspersoon probeert het slachtoffer zover te krijgen dat hij/zij een vrijblijvend/vertrouwelijk gesprek wil aangaan met de zedenrechercheur van de politie;
- Als het slachtoffer een gesprek wil wordt een afspraak gemaakt door de vertrouwenspersoon;
- Indien het slachtoffer absoluut geen gesprek met de politie wil wordt er een melding gedaan aan het Advies- en Meldpunt Kindermishandeling;
- De veiligheidscoördinator doet altijd melding bij de politie i.v.m. mogelijke professionele opvang slachtoffer, sporenonderzoek en medisch onderzoek;
- De veiligheidscoördinator informeert de leerjaarcoördinator/schoolleider van de afdeling waarin het slachtoffer les volgt.

Wat moet nooit gedaan worden:

- Het slachtoffer uithoren over datgene wat er is gebeurd. Volsta met datgene wat het slachtoffer spontaan vertelt;
- Ga geen gesprekken aan met personen die door het slachtoffer eerder in vertrouwen zijn genomen (vrienden en vriendinnen e.d.);
- Deze handelingen kunnen namelijk in een later stadium een getuigenverklaring onbruikbaar maken. Bij twijfel kan er altijd overlegd worden met een zedenrechercheur.

8. Vertrouwenspersonen (intern en extern)

Indien je op de werkvloer te maken hebt met ongewenst gedrag kun je hiervoor terecht bij een vertrouwenspersoon. Op dit moment wordt de functie van interne vertrouwenspersoon opnieuw uitgegeven.

Daarnaast is er een **extern vertrouwenspersoon** die je kunt raadplegen: Praatuit.nl. Het Jan Arentsz heeft Praatuit.nl ingehuurd om collega's ondersteuning en een luisterend oor te bieden in het geval van ongewenst gedrag op de werkvloer. Zij zijn te bereiken via:

- Whatsapp op 023-2010219 (op werkdagen tussen 9.00 en 21.00 uur binnen 1 uur een reactie)
- Telefonisch op 085-1071256 (op werkdagen tussen 9.00 en 21.00)
- Mail info@praatuit.nl.

Je kunt ook direct een afspraak maken voor het online spreekuur

9. Protocol camerabewaking

De schoolleiding van CSG Jan Arentsz vindt bescherming van eigendommen van de school en de schoolgebruiker belangrijk. Naast persoonlijke surveillance wordt gebruik gemaakt van camerabewaking in en rond de school.

Het doel van de camerabewaking is:

- Het beschermen van de schooleigendommen en de eigendommen van de gebruikers van de school;
- Preventie tegen vandalisme;
- Het bevorderen van het veiligheidsgevoel van de gebruikers van de school.

Gebruik van de camera:

- De camera's worden alleen gebruikt om te waken over de eigendommen en de veiligheid van de school en de schoolgebruiker;
- Bij de ingangen van het schoolterrein staan waarschuwingsborden met betrekking de camerabeveiliging.

Bewaren van de opgenomen informatie:

- De opgenomen informatie wordt één week bewaard op de harde schijf van het camerasysteem en daarna automatisch overschreven;
- De veiligheidscoördinator of een schoolleider kan opdracht geven de beelden op te slaan
- De veiligheidscoördinator bewaart deze beelden zolang hij nodig acht, echter niet langer dan één jaar. Dit in overleg met de vestigingsdirectie;
- De veiligheidscoördinator kan de CD ter beschikking stellen aan de politie. De politie dient daartoe de beelden schriftelijk te vorderen.

Het bekijken van de opgenomen beelden:

- Een bevoegde schoolfunctionaris mag bij het vermoeden van vandalisme, diefstal of een ander vergrijp de beelden bekijken om een mogelijke dader op te sporen. Deze kan de leerling of een collega toestemming geven mee te kijken;
- Bij een geweldsmisdrijf zal een bevoegde schoolfunctionaris de beelden bekijken om de mogelijke dader(s) te herkennen;
- In alle gevallen mogen de beelden alleen bekeken worden wanneer er een redelijke kans bestaat de mogelijke dader(s) te herkennen. Deze kan een slachtoffer of getuige toestemming geven om mee te kijken;
- Een bevoegde schoolfunctionaris is een medewerker die van de veiligheidscoördinator toestemming heeft de beelden te bekijken. Dit is Meinte Peterzon of Ivo Esser.
- De veiligheidscoördinator kan per incident anderen benoemen tot bevoegde schoolfunctionaris en deze toestemming geven de beelden zelfstandig te bekijken;
- De veiligheidscoördinator wordt altijd in kennis gesteld van wie de beelden heeft bekeken (leerling en/of medewerker) en wat het resultaat is geweest;
- De bevoegde schoolfunctionaris doet geen enkele mededeling, behalve aan de veiligheidscoördinator, vestigingsdirecteur of politie over datgene dat zichtbaar is op de beelden.

10. Het doen van aangifte op school

Bij diefstal of bij gebeurtenissen waar letsel en/of schade is toegebracht moet op het politiebureau aangifte gedaan worden. Wanneer de dader bekend is, wordt deze door de politie van school gehaald voor verhoor. Dit geeft in de school veel onrust. Vanuit het veiligheidsconvenant zijn werkafspraken gemaakt om in bepaalde gevallen aangifte op school op te nemen. Dit bevordert de rust op school. Ook wordt de totale tijdsduur erg ingekort, waardoor je meer een lik op stuk beleid krijgt, waardoor de dader(s) zich beter bewust worden van hun handelen. Wettelijke incidenten worden altijd geregistreerd in Magister.

POLITIE
Noord-Holland Noord

Werkproces opnemen aangiftes in school:

1. De veiligheidscoördinator of schoolleider neemt contact op met de jeugdcoördinator bij de politie;
2. Een aangifte met aansluitend een verhoor van eventuele getuigen en een verhoor van de verdachte(n) wordt alleen opgenomen met de jeugdcoördinator bij de politie en/of de schoolcontactagent;
3. Voordat de politie naar school komt kan de verdachte leerling worden nagetrokken in het politie-informatiesysteem bps. Bekend is dan of het gaat om een first offender;
4. De leerjaarcoördinatoren/schoolleiders van de afdeling(en) waar de betrokken leerlingen inzitten, informeren vooraf de ouders;
5. De school verschaft gelegenheid en middelen om de verhoren discreet plaats te laten vinden binnen de school;

6. De politie neemt:
   - De aangifte;
   - De getuige verklaringen;
   - En de verdachte verklaringen meteen op.

11. Handelingsprotocol bij ongewenst bezoek op het schoolterrein

De ongewenste persoon is bij de school bekend:

- Twee personeelsleden verzoeken de ongewenste persoon zich te verwijderen;
- Bij weigering wordt de ongewenste persoon gesommeerd te vertrekken;
- Bij weigering wordt deze sommering herhaald met de toevoeging dat anders de politie wordt gebeld;
- Bij weigering politie bellen;
- Overleg tussen de contactpersonen van de school en de politie;
- Indien ongewenst persoon terugkomt: wederom hetzelfde protocol hanteren.

De dader is bij de school niet bekend (zie hiervoor ook het protocol ongewenst bezoek op het schoolterrein):

- Wanneer er een melding binnenkomt zo veel mogelijk informatie vragen. Alle informatie noteren. Ook de naam van de melder noteren en na afloop terugkoppelen wat er gedaan is;
- Noteer datum en tijdstip van de melding;
- Altijd samen met (conciërge, schoolleiding lid of veiligheidscoördinator) gaan naar de plaats waar het probleem zich voordoet. Telefoon meenemen;
- Afspreken wie eventueel het (auto)nummer en signalement noteert en wie het woord voert;
- Wees in eerste instantie vriendelijk. Vraag eerst wat er aan de hand is. Vraag dan vriendelijk om te vertrekken, omdat het privé-terrein is. Zeg dan opnieuw dat het privé-terrein is en sommeer daarna om te vertrekken. Ga niet in discussie;
- Ga bij brutaliteit niet in discussie, maar loop rustig weg;
- Bel buiten zicht de politie en verwijs naar het convenant dat we hebben en noteer ook weer het tijdstip. Noteer ook wat er gezegd is;
- Politie opvangen en alle informatie doorgeven;
- Wanneer de politie niet komt eventueel achtergebleven sporen verzamelen. Raak hierbij niets met je handen aan (vingerafdrukken, gevaar voor AIDS) maar verzamel spullen met een pincet en doe alles in een plastic opbergzakje. Op het zakje datum en tijdstip noteren. Of vraag de veiligheidscoördinator dit te doen;
- Geef meteen na het gebeuren ook alle informatie en spullen aan de veiligheidscoördinator en/of vul het formulier in.

12. Zorgvuldig omgaan met informatie en sociale media

Vanwege het specifieke karakter (het grote bereik) van de social media is de bijlage opgedeeld in een algemeen deel, betreffende alle vastlegging van (persoons)informatie en een specifiek deel, betreffende social media.

12.1 Bewust 6x zorgvuldig omgaan met informatie

Als je persoonsgegevens deelt met anderen, dan moet je er op kunnen vertrouwen dat de ontvanger zorgvuldig met jouw gegevens omgaat. Als je werk met persoonsgegevens vraagt dit dan ook van medewerkers en leerlingen een aantal basisvaardigheden rondom het gebruiken en delen van persoonsgegevens. Dit vatten we samen als 'Bewust 6x Zorgvuldig'.

1. **Gebruik zorgvuldig: vergrendel je scherm**
   Verlaat je je werkplek om koffie te halen of wat anders, vergrendel je scherm. Niet alle informatie is voor iedereen bestemd. Windows-toets L vergrendelt direct je pc. Beveilig ook je privé PC met wachtwoord en virusscanner. Zorg dat je mobiele telefoon is voorzien van een toegangscode.

2. **Deel zorgvuldig: eerst denken, dan delen**
   Stel jezelf bewust de vraag welke gegevens ga ik delen, is dat niet te veel, kan het met minder gegevens. Zijn er alternatieven. Met wie deel ik de gegevens, mogen zij alles hebben. Gebruik het BCC veld bij een mail naar meerdere personen, groepen, organisaties. Vermijd discussies met leerlingen, ouders/verzorgers of derden op digitale media (nodig ze zo nodig uit voor een persoonlijk gesprek). Het is docenten niet toegestaan een whats app groep te starten met het oog op het ervaren verplichtende karakter wanneer het initiatief van school uitgaat. Dit is ongewenst in het kader van de wet op de privacy. Gebruik een alternatief.

3. **Surf zorgvuldig: klik niet klakkeloos**
   Denk vooraf goed na voor je klikt op een link in de mail of op een website, wees je bewust van eventuele gevaren als *ransomware* enz.

4. **Beveilig zorgvuldig: je wachtwoord is persoonlijk, deze leen je dus niet uit**
   - Kies een sterk wachtwoord
   - Vervang ze regelmatig.
   - Bewaar ze op een veilige plek.
   - Geef ze nooit aan iemand anders.

5. **Verbind zorgvuldig: check veilige verbinding**
   Vermijd gratis wifi mogelijkheden, check veilige verbindingen in de browser (o.a. groen slotje).
   School voorziet in de juiste gegevenstoegang om veilig met persoonsgegevens te werken.

6. **Sla zorgvuldig op**
   Gebruik bij voorkeur de toegestane cloud-opslag (Microsoft 365).

12.2 Zorgvuldig omgaan met social media

Wij besteden op school aandacht aan het leren omgaan met social media en leggen daarbij het verband met de bedoeling van ons onderwijs. Er is structureel aandacht voor het gebruik van social media in de lessen informatiekunde, projecten en in situaties waarin conflicten zijn die te maken hebben met social media.

Bij gebruik van social media zijn privé-gerelateerde en werk gerelateerde zaken niet zo gemakkelijk te scheiden. Medewerkers van Csg Jan Arentsz mogen actief zijn op social media mits het werk er niet onder lijdt. Het uitgangspunt bij het gebruik van social media door medewerkers is dat zij hiermee verstandig omgaan. Het gedrag op social media wijkt niet af van het levensechte gedrag binnen Csg Jan Arentsz.

Deze richtlijnen hebben te maken met situaties waarbij er een overlap is (of kan zijn) tussen werk en privé. Weblogs, fora en netwerken waar je alleen als privépersoon actief bent – over activiteiten die geen raakvlak hebben met de werksituatie – vallen hier expliciet niet onder.

Richtlijnen gebruik social media

1. Medewerkers proberen kennis en andere waardevolle informatie te delen, mits die informatie niet vertrouwelijk is en Csg Jan Arentsz niet schaadt.
2. Medewerkers kunnen zich mengen in discussies op social media over onderwijszaken. Dit kan op basis van persoonlijke ervaringen. Als een standpunt van Csg Jan Arentsz gepubliceerd wordt, vermeldt de schrijver dit.
3. Voor het publiceren van gesprekken, foto's, filmpjes wordt eerst expliciete schriftelijke toestemming gevraagd aan de betrokkenen (of ouders/voogd). Deze toestemming dient te worden bewaard in het personeelsdossier of leerling dossier van betrokkenen;
4. Bij onderwijs-onderwerpen maken medewerkers duidelijk dat zij op persoonlijke titel publiceren, tenzij dit met toestemming van de schoolleiding gebeurt.
5. Medewerkers van Csg Jan Arentsz gaan niet in discussie met een leerling, ouder/verzorger of derde op social media of andere digitale media. Mocht er aanleiding toe bestaan wordt deze persoon uitgenodigd voor een gesprek. Wanneer een online discussie dreigt te ontsporen, of in het ergste geval al helemaal ontspoord is, neem dan direct contact op met de verantwoordelijke afdeling/persoon en overleg over de te volgen strategie
6. Wees je, als medewerker van Csg Jan Arentsz, bewust van het feit dat er al snel een relatie gelegd kan worden met je werkzaamheden voor de school – ook als je een privé- mening verkondigt.
7. Medewerkers van Csg Jan Arentsz zijn persoonlijk verantwoordelijk voor wat zij publiceren.
8. Medewerkers van Csg Jan Arentsz zijn zich ervan bewust dat publicaties op social media altijd vindbaar zijn.
9. Bij twijfel over een publicatie overleggen medewerkers met collega's of leidinggevende.
10. Csg Jan Arentsz zorgt ook digitaal voor een veilig klimaat en het gedrag van medewerkers op social media wijkt niet af van wat in de klas en op school gebruikelijk is.
11. Leerlingen die op social media het veilige klimaat op Csg Jan Arentsz 'in gevaar' brengen worden daarop aangesproken.
12. In lessen wordt aandacht besteed aan het gebruik van social media door leerlingen en indien er een aanleiding toe is wordt er extra aandacht aan besteed.

13. Csg Jan Arentsz neemt bij overtreding van digitale omgangsvormen dezelfde maatregelen als bij overtreding van mondelinge of schriftelijke omgangsvormen.

12.3 Mobiele telefoons: thuis of in de kluis, telefoonbeleid voor leerlingen

Tijdens de lessen berg je je telefoon op in je kluisje of je laat de telefoon helemaal thuis.

Wat gebeurt er als je je telefoon toch bij je hebt in de les?
De eerste keer: je krijgt een herinnering aan de afspraak.
De tweede keer: je telefoon wordt tijdelijk bewaard en je kunt hem aan het einde van de dag ophalen op een centrale plek binnen de school.

Als je je telefoon meeneemt wees je er dan van bewust dat de school niet verantwoordelijk is voor beschadiging, verlies of diefstal. We raden je daarom aan om goed op je spullen te letten. Uitzonderingen worden individueel in overleg met de schoolleiding bepaald.

Csg Jan Arentsz heeft een verantwoordelijkheid als het gaat om de veiligheid van leerlingen en personeel. Dat begint met duidelijke en gecommuniceerde normen en waarden en de handhaving daarvan, ook digitaal. Daarom hanteert Csg Jan Arentsz duidelijke regels over het gebruik van computer devices.

- Computer devices dienen uit te staan tijdens de lessen tenzij de docent heeft aangegeven
  dat de computer devicer tijdens de les mag worden gebruikt;
- Aan leerlingen die computer devices ongeoorloofd gebruiken en/of zich norm overschrijdend gedragen zullen de gebruikelijke sancties (zie leerlingenstatuut en schoolreglement) worden opgelegd;
- Bij ongeoorloofd gebruik of norm overschrijdend gedrag worden de ouders/ vertegenwoordigers ingelicht. Gedacht kan worden aan kleineren van medewerkers of leerlingen via YouTube, dreigtweets, digitaal pesten en/of seksuele intimidatie;
- De schoolleider bepaalt wanneer het norm overschrijdend gedrag zodanig is dat de politie dient te worden ingeschakeld. Dit gebeurt in ieder geval als er sprake is van bedreiging.
- Bij ongeoorloofd of norm overschrijdend gedrag wordt de veiligheidscoördinator op de hoogte gebracht.
- Als er sprake is van aanwijsbare slachtoffers van eventueel norm overschrijdend gedrag wordt hen zo nodig hulp aangeboden;
- Als het norm overschrijdend gedrag leidt tot media-aandacht wordt de pers door de betreffende vestigingsdirecteur of, in geval van ernstige incidenten, de voorzitter college van bestuur te woord gestaan.

13. Procedure melding datalekken

Inleiding
Onze school is verplicht om datalekken in of hacks van systemen te melden.
Datalekken moeten gemeld worden bij de Autoriteit Persoonsgegevens in de volgende gevallen:

- Als een data lek is geconstateerd in een geautomatiseerd gegevensbestand waarvoor Csg Jan Arentsz verantwoordelijk is en wat gegevens bevat die tot een persoon (leerling, ouder/verzorger, medewerker of ander, aan school gerelateerd persoon) herleidbaar zijn.
- Bij verlies en/of ongeautoriseerde toegang tot een informatie systeem/computer device (zoals: laptop, mobiele telefoon, etc) dat gegevens bevat die tot een persoon (leerling, ouder/verzorger, medewerker of ander, aan school gerelateerd persoon) herleidbaar zijn.
- Indien er sprake is van een inbreuk op de beveiliging van persoonsgegevens die leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van de persoonsgegevens.

  NB: Als het datalek of de hack gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene(n), moet het ook aan hen gemeld worden.

De rol van externe partijen
Veel van de persoonsgegevens worden door medewerkers in de schoolomgeving geregistreerd en bewaard. Een groot deel van de registratie vindt echter bij externe leveranciers plaats. Deze leveranciers zijn schriftelijk op de hoogte gesteld van hun verplichting om een mogelijk lekken van data m.b.t. Csg Jan Arentsz direct na constatering te melden bij de applicatiebeheerder.

Bronsystemen bij externe partijen waarvan datalekken binnen 2 werkdagen gemeld moeten
worden aan de Autoriteit persoonsgegevens zijn:

a. Leerlingadministratiesysteem Magister, inclusief:
   I. Facet – digitale toetsing voor Rekentoetsen, CSPE's, DTT-pilot en CE's in VMBO
   II. OSO – beveiligde uitwisseling leerlingendossiers tussen PO en VO
   III. TOPdossier, wordt binnenkort ingevoerd t.b.v. beveiligde informatie-overdracht zorgleerlingen.
b. Personeelsadministratiesysteem AFAS
c. Databases van uitgevers waarin leerlinginformatie is opgeslagen

Andere informatiesystemen bij externe partijen die mogelijk datalekken kunnen veroorzaken of daar debet aan kunnen zijn:

d. Entree-koppelingen (ook naar de methodensites) vanuit Magister
e. Microsoft Azure Active Directory-koppelingen en Google Suite for Education-koppelingen
f. Bookmaster, het registratiesysteem van de boeken-/licentieleverancier

Signalering, melding en escalatie van datalekken

- Signalering van datalekken is belegd bij de functioneel beheerders van de systemen. Dit zijn de personen die bij uitstek als een van de eersten op de hoogte zijn van een mogelijk datalek in zo'n systeem.

- Ook alle andere medewerkers die gebruik maken van gegevensdragers zijn verplicht om een datalek in hun gegevensdrager te melden.
- Bij de signalering van een datalek meldt de functioneel beheerder (of de medewerker die het betreft) dit direct bij de veiligheidscoördinator. Tevens registreert de functioneel beheerder het datalek in het incidentenregistratiesysteem van Magister
- De veiligheidscoördinator verricht een beoordeling conform de eisen van de wet- en regelgeving (Algemene verordening gegevensbescherming).
- De veiligheidscoördinator bespreekt de beoordeling met het bevoegd gezag (voorzitter CvB).
- Als het datalek valt in de categorieën zoals in de inleiding gesteld meldt de veiligheidscoördinator dit namens het bevoegd gezag bij de Autoriteit persoonsgegevens. Dit gebeurt via het digitale meldloket van de autoriteit persoonsgegevens.
- Als het datalek of de hack gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene(n), meldt de veiligheidscoördinator dit ook aan hen.
- De veiligheidscoördinator vult de melding in het incidentenregistratiesysteem aan met de ondernomen acties.

14. Informatiebeveiliging en privacy beleid

14.1 HET BELANG VAN INFORMATIEBEVEILIGING EN PRIVACY

Het onderwijs is in toenemende mate afhankelijk van informatie en ICT. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door o.a. ontwikkelingen als gepersonaliseerd leren met ICT. Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. De afhankelijkheid van ICT en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het goed regelen van informatiebeveiliging en privacy (afgekort tot IBP) in een IBP-beleid is noodzakelijk om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

14.1.1. Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een hoeveelheid samenhangende maatregelen zodat de betrouwbaarheid van de informatievoorziening gegarandeerd kan worden.
Informatiebeveiliging richt zich op de volgende aspecten:
Beschikbaarheid: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
Integriteit: de mate waarin gegevens en/of functionaliteiten juist en volledig zijn.
Vertrouwelijkheid: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

Onvoldoende informatiebeveiliging kan leiden tot ongewenste risico's in het onderwijsproces en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

14.1.2. Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de huidige wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die een natuurlijke persoon direct of indirect kunnen identificeren. Onder verwerking wordt elke handeling met betrekking tot persoonsgegevens verstaan. De wet noemt als voorbeelden van verwerking:
Het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.

14.1.3. Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijke voorwaarde is voor privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk, en worden daarom samengevoegd tot één proces: IBP. Dit beleid, verder te benoemen als IBP-beleid, vormt de basis op informatiebeveiliging en privacy binnen Stichting christelijk voortgezet onderwijs Alkmaar e.o. te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

14.2 DOEL

Informatiebeveiliging en privacy heeft de volgende doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen waarvan Stichting christelijk voortgezet onderwijs Alkmaar e.o. persoonsgegevens verwerkt, waaronder leerlingen, hun ouders/verzorgers en medewerkers
- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

Het informatiebeveiligings- en privacy beleid (IBP-beleid) is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een juiste balans moet zijn tussen privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene (o.a. medewerkers, leerlingen en hun ouders/verzorgers) wordt gerespecteerd en Stichting christelijk voortgezet onderwijs Alkmaar e.o. voldoet aan relevante wet- en regelgeving.

14.3 REIKWIJDTE

- Het IBP-beleid binnen Stichting christelijk voortgezet onderwijs Alkmaar e.o. geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing). Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.
- Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Stichting christelijk voortgezet onderwijs Alkmaar e.o. waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan Stichting christelijk voortgezet onderwijs Alkmaar e.o. persoonsgegevens verwerkt.
- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van Stichting christelijk voortgezet onderwijs Alkmaar e.o. Hieronder valt tevens de gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop de school kan worden aangesproken. (b.v. uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites en of social media.)
- Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van Stichting christelijk voortgezet onderwijs Alkmaar e.o. evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het IBP-beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

- IBP-beleid heeft binnen Stichting christelijk voortgezet onderwijs Alkmaar e.o.

raakvlakken met:

- *Algemeen veiligheids- en toegangsbeveiligingsbeleid;* met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen
- *Personeels- en organisatiebeleid;* met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties
- *IT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ict en (digitale) leermiddelen
- *Medezeggenschap* van leerlingen, hun ouders/verzorgers en medewerkers

14.4 BELEID – Hoe doen we dat?

Stichting christelijk voortgezet onderwijs Alkmaar e.o. hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het schoolbestuur van Stichting christelijk voortgezet onderwijs Alkmaar e.o. neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de verwerkingsverantwoordelijke.
2. Stichting christelijk voortgezet onderwijs Alkmaar e.o. voldoet aan alle relevante wet- en regelgeving.
3. Bij Stichting christelijk voortgezet onderwijs Alkmaar e.o. is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen. Een goede balans tussen het belang van Stichting christelijk voortgezet onderwijs Alkmaar e.o. om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot het gebruik van zijn/haar persoonsgegevens is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen ten alle tijden hun toestemming herzien.
4. Stichting christelijk voortgezet onderwijs Alkmaar e.o. zal alle betrokkenen helder en actief informeren over de verwerkingen van hun persoonsgegevens, die zowel direct als indirect zijn verkregen. Ook worden alle betrokkenen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit en profilering.
5. Stichting christelijk voortgezet onderwijs Alkmaar e.o. legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. Stichting christelijk voortgezet onderwijs Alkmaar e.o. voldoet hiermee aan de documentatieplicht.
6. Binnen Stichting christelijk voortgezet onderwijs Alkmaar e.o. is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van papieren documenten.
7. Stichting christelijk voortgezet onderwijs Alkmaar e.o. is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.

8. Stichting christelijk voortgezet onderwijs Alkmaar e.o. classificeert informatie en informatiesystemen. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen maatregelen. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen en de te nemen maatregelen.
9. Stichting christelijk voortgezet onderwijs Alkmaar e.o. sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de school, persoonsgegevens verwerken. Dit geldt ook voor andere organisaties indien er gegevens van leerlingen of medewerkers worden verstrekt.
10. Stichting christelijk voortgezet onderwijs Alkmaar e.o. verwacht van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. Stichting christelijk voortgezet onderwijs Alkmaar e.o. heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.
11. Informatiebeveiliging en privacy is bij Stichting christelijk voortgezet onderwijs Alkmaar e.o. een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
12. Stichting christelijk voortgezet onderwijs Alkmaar e.o. kijkt bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen vóóraf naar de impact hiervan op de informatiebeveiliging en privacy, zodat tijdig de juiste maatregelen genomen kunnen worden.
13. Stichting christelijk voortgezet onderwijs Alkmaar e.o. neemt passende technische (beveiligings-)maatregelen om persoonsgegevens en overige data te beschermen tegen de risico's, die de voortgang van het onderwijs, de privacy en de bedrijfsvoering kunnen verstoren.
    Optioneel: Als de infrastructuur elders wordt beheerd en/of gegevens elders worden verwerkt legt Stichting christelijk voortgezet onderwijs Alkmaar e.o. aanvullende afspraken vast over de technische maatregelen.
14. Stichting christelijk voortgezet onderwijs Alkmaar e.o. zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen

14.5 UITWERKING VAN HET BELEID– Wat doen we?

Dit hoofdstuk geeft een praktische invulling van bovenstaande beleidspunten en is daarmee de minimale invulling van het beleid.

14.6 RELEVANTE WET- EN REGELGEVING

De uitwerking van het beleid voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs en/of Wet op de expertisecentra
- Wet goed onderwijs en goed bestuur PO/VO
- Wet onderwijstoezicht
- Wet bescherming persoonsgegevens (Wbp; tot 25 mei 2018)
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)*
- Archiefwet
- Leerplichtwet

- Auteurswet
- Wetboek van Strafrecht

De internationale norm voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2015) is leidend voor de te nemen beveiligingsmaatregelen.

De bepalingen van de meest recente versie van het convenant 'Digitale onderwijsmiddelen en privacy' zijn leidend bij het maken van afspraken met leveranciers, die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerken.

14.7 BASISREGELS BIJ HET OMGAAN MET PERSOONSGEGEVENS

Bij het verwerken van persoonsgegevens zijn de wettelijke beginselen inzake verwerking persoonsgegevens (art.5 AVG) leidend. Deze zijn samengevat in de vijf vuistregels met betrekking tot de omgang met persoonsgegevens te weten.

14.7.1 Doelbepaling en doelbinding:
persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.

14.7.2 Grondslag:
verwerking van persoonsgegevens is gebaseerd op een van de zes wettelijke grondslagen.

14.7.3 Dataminimalisatie:
bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding staan tot het doel (proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt (subsidiair). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.

14.7.4 Transparantie:
de school legt aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IBP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Tevens kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.

14.7.5 Data-integriteit:
er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

14.8 ONDERSTEUNENDE RICHTLIJNEN EN PROCEDURES

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Bijlage 1 geeft een overzicht van de

diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister.

14.9 VOORLICHTING EN BEWUSTZIJN

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens is hier een belangrijke factor. Daarom wordt het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, leerlingen en gasten. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de verantwoordelijke IBP, de FG, en de Security Officer met het bestuur als eindverantwoordelijke.

14.10 CLASSIFICATIE EN RISICOANALYSE

Alle informatie heeft waarde, daarom worden alle gegevens en informatiesystemen waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de te nemen beveiligingsmaatregelen is afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de betrouwbaarheidsaspecten die van belang zijn.
Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt vóóraf gekeken naar de impact van de ontwikkelingen en de beoogde verwerkingen op informatiebeveiliging en privacy, zodat passende maatregelen genomen kunnen worden. Vanaf de start van nieuwe (ict)projecten wordt rekening gehouden met informatiebeveiliging en privacy.

14.11 INCIDENTEN EN DATALEKKEN

Alle medewerkers, die een beveiligingsincident of datalek vermoeden dienen dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in een protocol. De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle (beveiligings)incidenten worden vastgelegd in een incidentenregister. Alle (beveiligings)incidenten kunnen worden gemeld bij <mailbox/ helpdesk/ medewerker>.
Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

14.12 PLANNING EN CONTROLE

Dit IBP-beleid wordt minimaal elke twee jaar getoetst en bijgesteld door het bestuur. Hierbij wordt rekening gehouden met:

- De status van de informatiebeveiliging als geheel (beleid, organisatie, risico's);
- de actuele geïnventariseerde risico's;
- de effectiviteit van de genomen maatregelen en aantoonbare werking daarvan

Daarnaast kent Stichting christelijk voortgezet onderwijs Alkmaar e.o. een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings-

en privacy beleid wordt getoetst. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving et cetera meegenomen.

14.13 NALEVING EN SANCTIES

De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid en richtlijnen. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode, met periodieke bewustwordingscampagnes, et cetera.
Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door de het bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het bestuur vast te stellen reglement.

Mocht de naleving van dit beleid ernstig tekort schieten, dan kan Stichting christelijk voortgezet onderwijs Alkmaar e.o. de betrokken verantwoordelijke medewerkers een sanctie op leggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

14.14 LOGGING EN MONITORING

Logging en monitoring door de IT-afdeling zorgt er voor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens wordt vastgelegd. Hieronder vallen onder andere het in- uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk.

14.15 ORGANISATIE - Wie doet wat?

14.15.1 Rollen en verantwoordelijkheden

De organisatie van IBP gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol. Onderstaand overzicht geeft aan welke verantwoordelijkheden en taken bij welke rollen horen bij Stichting christelijk voortgezet onderwijs Alkmaar e.o..

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richtinggevend (strategisch)	Voorbeelden: CvB	• Eindverantwoordelijk • IBP-beleidsvorming, -vastlegging en het uitdragen ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Evalueren toepassing en werking IBP-beleid op basis van rapportages • Organisatie IBP inrichten	• Informatiebeveiligings- en privacy beleid • Baseline / basismaatregelen • Reglement FG vaststellen • Privacyreglement vaststellen
	Kernteam IBP: ICT specialist Functioneel beheerder Hoofd bedrijfsvoering	• Inhoudelijk verantwoordelijk voor IBP • IBP-planning en controle • Adviseert bestuur/CvB/directie over IBP • Voorbereiden uitvoeren IBP-beleid, Classificatie/risicoanalyse • Hanteren IBP normen en wijze van toetsen • Evalueren IBP-beleid en maatregelen • Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze • Schrijven en beheren van processen, richtlijnen en	Processen, richtlijnen en procedures IBP, waaronder: • activiteitenkalender • Protocol beveiligingsincidenten en datalekken • Verwerkersovereenkomsten regelen • Brief toestemming gebruik beeldmateriaal • Opstellen informatie documentatie richting leerlingen, ouders / verzorgers • Security awareness activiteiten • Sociale media reglement • Gedragscode ict en internetgebruik • Gedragscode medewerkers en leerlingen

		procedures om de uitvoering te ondersteunen	
	Functionaris voor Gegevensbescherming en/of Privacy officer	• Toezicht op naleving privacy wetgeving • Voorlichting privacy en stimuleren bewustwording • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Afwikkeling klachten en incidenten	• Privacyreglement, • procedure IBP-incident afhandeling • Inrichten meldpunt datalekken
	Domeinverantwoordelijke/ Proceseigenaren Waaronder o.a.: ICT, HRM / P&O, facilitair, onderwijs, financiën en administratie	• **Classificatie / risicoanalyse** in samenwerking met kernteam • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door bestuur/CvB/schoolleiding • Samen met functioneel beheer en ICT beheer er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. • Samen met functioneel beheer en ICT beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren.	• Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst); input dataregister • Classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk

Uitvoerend (operationeel)	Security officer (ict specialist)	• Incidentafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor IBP-incidenten.	
	Functioneel en/of applicatie beheerder	• Uitvoeren taken conform gegeven richtlijnen en procedures.	
	Medewerker	• Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden.	Communiceren, informeren en toezien op naleving van o.a.: • IBP in het algemeen • Regels passend onderwijs • Hoe omgaan met leerling dossiers • Wie mogen wat zien • Gedragscode • Omgaan met sociale media • Mediawijs maken
	Stafhoofden / schoolleiding	• Communicatie naar alle betrokkenen; er voor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan. • Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers. • Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid. • Implementeren IBP-maatregelen. • periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.; • Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan bestuur.	

De verdere uitwerking van de rollen en taken staan beschreven in bijlage 2.

Informatiebeveiliging en privacy beleid

Bijlage 1: Ondersteunende richtlijnen en procedures

Deze bijlage bevat een aantal aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Een aantal zijn vanuit de Algemene Verordening Gegevensbescherming verplicht.

Documenten:	**Aandachtspunten:**
Procedure toestemming gebruik beeldmateriaal	(toestemmingsbrief)
Procedure voor verwijderen van gegevens	(bewaartermijnen)
Communicatie rechten betrokkenen	(communicatie richting betrokkenen)
Procesbeschrijving rechten betrokkenen	(proces rondom aanvragen van betrokkenen)
Privacyreglement	
Autorisatiematrix	(wie mogen gegevens inzien, bewerken enz.)
Afspraken gebruik sociale media	
Procedure rondom training medewerkers	(bewustzijn creëren)
Cameratoezicht	
Wachtwoordbeleid	
Responsible disclosure	
Gedragscode ict en internetgebruik	
Acceptable use policy	(verantwoord gebruik bedrijfsmiddelen)
Procedure rondom uitwisselen gegevens	(passend onderwijs, leerling dossiers, leerplicht enz)

Verplicht vanuit de AVG:

Procesbeschrijving melden datalekken	
Registratie beveiligingsincidenten	
Dataregister om te voldoen aan de registratieplicht	
Verwerkersovereenkomsten	(privacy bijlage beschikbaar stellen)
Procedure gegevensbeschermingseffectbeoordeling	(DPIA)
Risicoanalyse	
Functionaris voor Gegevensbescherming	

Informatiebeveiliging en privacy beleid

Bijlage 2: Organisatie; wie doet wat

Deze bijlage beschrijft hoe IBP op drie niveaus wordt georganiseerd.

- Richtinggevend (strategisch)
- Sturend (tactisch)
- Uitvoerend (operationeel)

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij Stichting christelijk voortgezet onderwijs Alkmaar e.o. voor elk niveau een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen.
Beschreven wordt welke rollen, welke verantwoordelijkheden en taken hebben en wat de documenten zijn die daarbij passen.

Richtinggevend

Voorzitter college van bestuur
Het schoolbestuur / College van Bestuur/ directie is eindverantwoordelijk voor IBP en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast.
De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages geëvalueerd.
De inhoudelijke verantwoordelijkheid voor IBP is gemandateerd aan de manager IBP.

Sturend

Hoofd bedrijfsvoering
Manager IBP (verantwoordelijke IBP, informatiemanager of privacy officer) is een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke (het bestuur) en stuurt de mensen aan op uitvoerend niveau. De manager IBP moet:

- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling
- De uniformiteit bewaken binnen Stichting christelijk voortgezet onderwijs Alkmaar e.o.
- Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy
- De verdere afhandeling van incidenten binnen Stichting christelijk voortgezet onderwijs Alkmaar e.o. coördineren

Functionaris voor Gegevensbescherming of Privacy Officer
De functionaris voor gegevensbescherming (FG), of Privacy Officer indien er geen FG is aangesteld, houdt binnen Stichting christelijk voortgezet onderwijs Alkmaar e.o. toezicht op de toepassing en naleving van de AVG. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. De FG zorgt voor het verbeteren en stimuleren van bewustwording rondom IBP, het afhandelen van informatiebeveiligingsincidenten, adviseert over het regelen van privacy, onderhoudt zo nodig de contacten met de Autoriteit Persoonsgegevens (AP) en rapporteert aan de eindverantwoordelijke (voorzitter college van bestuur). De FG heeft regelmatig overleg met het hoofd bedrijfsvoering. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen.

ICT specialist en functioneel beheerder

Adviseert samen met hoofd bedrijfsvoering de voorzitter van het college van bestuur en is verantwoordelijk voor het organiseren van ICT en informatiebeveiliging binnen Stichting christelijk voortgezet onderwijs Alkmaar e.o.

Optioneel:
Portefeuillehouder informatiebeveiliging
Het management lid dat ICT en informatiebeveiliging / privacy in zijn portefeuille heeft is gesprekspartner voor de manager IBP in kader van informatiebeveiliging en privacy binnen de organisatie.

Domeinverantwoordelijke / proceseigenaar
Binnen de school zijn er verschillende domeinen/processen, zoals ict, personeel (HRM, P&O), administratie, facilitaire- en financiële zaken, onderwijs et cetera. Op elk van deze domeinen/processen is iemand verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.

Deze proceseigenaar is tevens verantwoordelijk voor de risico's die veroorzaakt worden doordat personen of applicaties ten onrechte toegang krijgen tot applicaties. Om deze risico's te verkleinen hebben proceseigenaren de volgende specifieke taken:
- Samen met de eindverantwoordelijke stellen zij het beleid voor toegang (autorisaties) vast.
- Samen met functioneel beheer en ICT-beheer zien zij er op toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn en voor hun werkzaamheden toegang toe moeten hebben.
- Samen met functioneel beheer en ICT-beheer beoordelen zij periodiek de toegangsrechten van de gebruikers.

Uitvoerend

Specialist ICT
De Security Officer vormt een technisch aanspreekpunt als het gaat over informatiebeveiliging voor het management en de medewerkers.

Functioneel beheerder of Applicatiebeheerder
Ieder softwarepakket of (web-)applicatie heeft een beheerder. Bij vragen over de software of applicatie is bekend wie daarvoor aangesproken kan worden. De functioneel beheerder wordt vanuit de domeinverantwoordelijke / proceseigenaar voorzien van een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert hij zijn of haar taken uit.
.
Medewerker
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. het personeelshandboek en de handleiding acceptabel gebruikmaken van bedrijfsmiddelen. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.

Medewerkers worden gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van security incidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de MR)

Stafhoofden en schoolleiders
Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft op uitvoerend niveau de taak om:

- ervoor te zorgen dat zijn medewerkers op de hoogte zijn van het IBP-beleid;
- toe te zien op de naleving van het IBP-beleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft;
- periodiek het onderwerp IBP onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;
- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde IBP-onderwerpen.

De leidinggevende kan in zijn taak ondersteund worden door de manager IBP. Leidinggevenden hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.

Kernteam IBP
Het kernteam IBP wordt organisatie breed zowel preventief als curatief benoemd voor informatiebeveiliging en privacy incidenten. De leden van het kernteam IBP zijn benoemd door de eindverantwoordelijke en handelen in diens opdracht.
Het IBP-team van Stichting christelijk voortgezet onderwijs Alkmaar e.o. heeft de volgende opdracht:

- Het signaleren en registreren van alle privacy verzoeken, beveiligingsincidenten en datalekken. Het coördineren van de maatregelen en het toezien op de oplossing van problemen die tot incidenten hebben geleid of waardoor de incidenten zijn veroorzaakt (of het bieden van ondersteuning daarbij);
- Het geven van voorlichting en het doen van algemene aanbevelingen aan netwerkbeheerders, systeembeheerders, ontwikkelaars en eindgebruikers door het verspreiden van informatie;
- Het leveren van managementrapportages en verbetervoorstellen aan de domeinverantwoordelijke/proceseigenaren over de beveiligingsincidenten en verzoeken tot uitoefening privacyrechten van de betrokkenen.

Bij een calamiteit kan het kernteam IBP terstond bij elkaar worden geroepen op initiatief van het hoofd bedrijfsvoering, in opdracht van het Stichting christelijk voortgezet onderwijs Alkmaar e.o.. Het doel hiervan is om de **continuïteit** van de informatievoorziening en de privacy te waarborgen. Onder calamiteiten worden verstaan:

- Datalek;
- Grote verstoringen van het netwerk (bijvoorbeeld DDoS aanval);
- Natuurrampen (brand, overstroming, storm, etc.).

Voor situaties als bovenstaand beschreven is een crisisplan beschikbaar welke gevolgd dient te worden!

Het IBP-team bij Stichting christelijk voortgezet onderwijs Alkmaar e.o. behandelt meldingen vertrouwelijk en verstrekt alleen informatie over beveiliging en privacy incidenten als dat noodzakelijk en relevant is voor de oplossing van een incident.
De werkzaamheden van het IBP-team bij Stichting christelijk voortgezet onderwijs Alkmaar e.o. is gedocumenteerd en door de eindverantwoordelijke bekrachtigd.

15. Privacyreglement CSG Jan Arentsz

1. Definities:	
Persoonsgegevens	Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;
Verwerking van persoonsgegevens	Eke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;
Bijzonder Persoonsgegeven	Een persoonsgegeven dat iets zegt over iemand zijn godsdienst, levensovertuiging, ras, politieke gezindheid of zijn gezondheid;
Betrokkene	Degene op wie een persoonsgegeven betrekking heeft al dan niet vertegenwoordigd door diens wettelijk vertegenwoordiger. In dit reglement gaat het om de leerlingen en de medewerkers**;**
Wettelijk vertegenwoordiger	Indien de betrokkene de leeftijd van zestien jaren nog niet heeft bereikt, wordt de betrokkene vertegenwoordigd door zijn wettelijk vertegenwoordiger. Meestal zal dit een ouder zijn maar het kan hier ook gaan om een voogd;
Verantwoordelijke	De verantwoordelijke stelt vast welke persoonsgegevens er verwerkt worden én wat het doel is van die verwerking. Dit is de rechtspersoon waar de Csg Jan Arentsz onder valt, vertegenwoordigd door het bevoegd gezag.
Bewerker	Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;
Derde	Ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken;
School	De verantwoordelijke onderwijsinstelling / bevoegd gezag van Csg Jan Arentsz
2. Reikwijdte en doelstelling	1. Dit reglement stelt regels over de verwerking van persoonsgegevens van leerlingen en medewerkers van Csg Jan Arentsz. 2. Dit reglement is van toepassing op alle persoonsgegevens van de betrokkene die door Csg Jan Arentsz worden verwerkt.

	Dit reglement heeft tot doel: a. de persoonlijke levenssfeer van de betrokkenen te beschermen tegen verkeerd en onbedoeld gebruik van de persoonsgegevens; b. vast te stellen welke persoonsgegevens worden verwerkt en met welk doel dit gebeurt; c. de zorgvuldige verwerking van persoonsgegevens te waarborgen; d. de rechten van betrokkene te waarborgen.
3. Doelen v/d verwerking van de persoonsgegevens	Bij de verwerking van persoonsgegevens houdt Csg Jan Arentsz zich aan de relevante wetgeving waaronder de Algemene verordening gegevensbescherming.
Doelen	De verwerking van persoonsgegevens vindt plaats voor de doelen zoals beschreven in de bijlagen 1, 2 en 3.
4. Doelbinding	Persoonsgegevens worden uitsluitend gebruikt voor zover dat gebruik verenigbaar is met de omschreven doelen van de verwerking. Csg Jan Arentsz verwerkt niet meer gegevens dan noodzakelijk is om die vastgestelde doelen te bereiken.
5. Soorten gegevens	De door de Csg Jan Arentsz gebruikte categorieën van persoonsgegevens worden in de bijlagen opgesomd.
6. Grondslag Verwerking	Verwerking van persoonsgegevens gebeurt alleen op grond van: a. Toestemming: in het geval de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend b. Overeenkomst: in het geval de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst c. Wettelijke verplichting: in het geval de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan Csg Jan Arentsz onderworpen is d. Vitaal belang: e. Publiekrechtelijke taak: in het geval de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens

	worden verstrekt f. Gerechtvaardigd belang.
7. Bewaartermijnen	Csg Jan Arentsz bewaart de gegevens niet langer dan dat zij noodzakelijk zijn voor het vervullen van het doel waarvoor zij zijn verkregen, tenzij er een andere wettelijke verplichting is die het langer bewaren van de gegevens verplicht stelt.
8. Toegang	Csg Jan Arentsz verleent slechts toegang tot de in de administratie en systemen van Csg Jan Arentsz opgenomen persoonsgegevens aan: a. de bewerker en de derde die onder rechtstreeks gezag van Csg Jan Arentsz staat; b. de bewerker die gemachtigd is om persoonsgegevens te verwerken; c. derden die op grond van de wet toegang moet worden verleend, waarbij alleen toegang wordt verleend aan de gegevens waartoe volgens de wet toegang toe moet worden gegeven.
9. Beveiliging en geheimhouding	a. Csg Jan Arentsz neemt passende technische en organisatorische beveiligingsmaatregelen om te voorkomen dat de persoonsgegevens worden beschadigd, verloren gaan of onrechtmatig worden verwerkt. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen. b. Csg Jan Arentsz zorgt dat medewerkers niet meer inzage of toegang hebben tot de persoonsgegevens dan zij strikt noodzakelijk nodig hebben voor de goede uitoefening van hun werk. c. Bij de beveiligingsmaatregelen wordt rekening gehouden met de stand van de techniek en de kosten van de tenuitvoerlegging. Daarbij houdt Csg Jan Arentsz rekening met de concrete risico's die van toepassing kunnen zijn op de verwerkte persoonsgegevens. d. Iedereen die betrokken is bij de uitvoering van dit reglement, en daarbij de beschikking krijgt over persoonsgegevens die vertrouwelijk zijn of geheim moeten worden gehouden (zoals bijvoorbeeld zorggegevens), en voor wie niet reeds uit hoofde van beroep, functie of wettelijk voorschrift een geheimhoudingsplicht geldt, is verplicht tot geheimhouding van

	die persoonsgegevens daarvan. e. De verantwoordelijke zal conform de Meldplicht datalekken de Autoriteit Persoonsgegevens onverwijld in kennis stellen van een inbreuk op de beveiliging die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. f. De verantwoordelijke zal conform de meldplicht datalekken de betrokkene onverwijld in kennis stellen van de inbreuk bedoeld onder e als de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. g. Een ieder die betrokken is bij de uitvoering van dit reglement en op de hoogte raakt van een (mogelijk) inbreuk op de beveiliging zoals bedoeld onder e is verplicht hiervan onverwijld melding te maken bij de verantwoordelijke. (via de veiligheidscoördinator, per e-mail).
10. Verstrekken gegevens aan derden	Gegevens worden slechts verstrekt aan derden indien de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend, de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is en/of de gegevensverwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene.
11. Sociale media	Voor het gebruik van persoonsgegevens in sociale media, zijn aparte afspraken gemaakt in het 'protocol zorgvuldig omgaan met informatie en sociale media' van Csg Jan Arentsz.
12. Rechten betrokkenen	De Algemene verordening gegevensbescherming geeft de betrokkene een aantal rechten. Csg Jan Arentsz erkent deze rechten en handelt in overeenstemming met deze rechten.
Inzage	a) Elke betrokkene heeft recht op inzage van de door Csg Jan Arentsz verwerkte persoonsgegevens die op hem/haar betrekking hebben. Csg Jan Arentsz kan vragen om een geldig identiteitsbewijs ter verificatie van de identiteit van de verzoeker
Verbetering, aanvulling, verwijdering en afscherming	b) Betrokkene kan een verzoeken doen tot verbetering, aanvulling, verwijdering of afscherming van zijn persoonsgegevens, tenzij er een wettelijke verplichting tot behoud van de gegevens is, dit onmogelijk blijkt of een onredelijke inspanning zou vergen.

Verzet	c) Voor zover Csg Jan Arentsz persoonsgegevens gebruikt op de grond van artikel 7 onder e en f, dan kan de betrokkene zich verzetten tegen verwerking van persoonsgegevens op basis van diens persoonlijke omstandigheden.
Termijn	d) Csg Jan Arentsz dient binnen een termijn van 4 weken na ontvangst van een verzoek daar schriftelijk gehoor aan te geven dan wel deze schriftelijk, gemotiveerd af te wijzen. Csg Jan Arentsz kan de betrokkene laten weten dat er meer tijd nodig is en deze termijn verlengen met maximaal 4 weken.
Uitvoeren verzoek	e) Indien het verzoek van de betrokkene wordt gehonoreerd, draagt Csg Jan Arentsz zorg voor het zo spoedig mogelijk doorvoeren van de verzochte wijzigingen.
Intrekken toestemming	f) Voor zover voor de verwerking van persoonsgegevens voorafgaande toestemming vereist is, kan deze toestemming te allen tijde door de wettelijk vertegenwoordiger worden ingetrokken.
13. Transparantie	1. Csg Jan Arentsz informeert de betrokkene over de verwerking van zijn persoonsgegevens. Indien het type verwerking dat vraagt, informeert de Csg Jan Arentsz iedere betrokkene apart over de details van die verwerking. 2. Csg Jan Arentsz informeert de betrokkene – op hoofdlijnen – ook over de afspraken die gemaakt zijn met derden en bewerkers die persoonsgegevens van de betrokkene ontvangen.
14. Klachten	1. Wanneer betrokkene van mening is dat het doen of nalaten van Csg Jan Arentsz niet in overeenstemming is met de wetgeving of dit reglement, dan kan betrokkene zich wenden tot het bevoegd gezag van Csg Jan Arentsz. 2. Overeenkomstig de Algemene verordening gegevensbescherming kan de betrokkene zich eveneens wenden tot de rechter of de Autoriteit Persoonsgegevens.
15. Onvoorziene situatie	Indien er zich een situatie voordoet die niet beschreven is in dit reglement dan neemt de verantwoordelijke de benodigde maatregelen rekening houdend met actuele wet- en regelgeving.
16. Wijzigingen reglement	Dit reglement wordt na instemming door de MR vastgesteld door de verantwoordelijke. De verantwoordelijke maakt dit reglement openbaar via de website van de school. De verantwoordelijke heeft het recht dit reglement, met instemming van de MR te wijzigingen.

17. Slotbepaling	Dit reglement wordt aangehaald als “het privacyreglement van Csg Jan Arentsz” en treedt voor de eerste keer in werking in februari 2018**.**

Privacyreglement CSG Jan Arentsz

Bijlage 1: Administratie leerlingen

1. De verwerking geschiedt slechts voor de volgende doelen:
   a. De organisatie of het geven van het onderwijs, de begeleiding van leerlingen, dan wel het geven van studieadviezen;
   b. Het verstrekken of ter beschikking stellen van leermiddelen;
   c. Het bekend maken van informatie over de organisatie en leermiddelen, bedoeld onder a en b, alsmede informatie over de leerlingen, bedoeld onder a, op de eigen website;
   d. Het bekendmaken van de activiteiten van de instelling op de eigen website;
   e. Het berekenen, vastleggen en innen van vrijwillige ouderbijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten, waaronder begrepen het in handen van derden stellen van vorderingen;
   f. Het behandelen van geschillen en het doen uitoefenen van accountantscontrole;
   g. Het onderhouden van contacten met de oud-leerlingen en oud-medewerkers van de verantwoordelijke;
   h. Andere dan de onder a tot en met g bedoelde gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van de geldende wet- en regelgeving.

2. Geen andere gegevens worden verwerkt dan:
   a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie bedoelde gegevens van de betrokkene;
   b. het persoonsgebonden nummer (BSN);
   c. nationaliteit en geboorteplaats;
   d. gegevens als bedoeld onder a, van de wettelijk vertegenwoordiger of verzorger van de leerling;
   e. gegevens betreffende de gezondheid of het welzijn van de leerling voor zover die noodzakelijk zijn voor passende ondersteuning;
   f. gegevens betreffende de godsdienst of levensovertuiging van de leerling, voor zover die noodzakelijk zijn voor de school, het onderwijs of de te geven ondersteuning;
   g. gegevens betreffende de aard en het verloop van het onderwijs en ondersteuning, alsmede de behaalde studieresultaten;
   h. schoolgegevens (waaronder naam school, naam zorgcoördinator/mentor/ intern begeleider, klas/groep waarin de leerling zit, tijdstip van inschrijving bij deze school, naam van de indiener van de aanmelding bij het samenwerkingsverband, schoolloopbaan en rapportage vanuit primair en voortgezet onderwijs);
   i. aanleiding voor de aanmelding bij het samenwerkingsverband, relevante screenings- en onderzoeksgegevens en omschrijving van de problematiek die aan de orde is;
   j. activiteiten die door de school zijn ondernomen rond de betreffende leerling, alsmede de resultaten hiervan;
   k. bestaande of (relevante) afgesloten hulpverleningscontacten en de namen van contactpersonen;
   l. relevante persoonsgegevens die door externe partijen worden verstrekt met betrekking tot de aangemelde problematiek van de betreffende leerling;
   m. relevante financiële gegevens over bijvoorbeeld de vrijwillige ouderbijdrage;

Privacyreglement CSG Jan Arentsz

Bijlage 2: Administratie Sollicitanten

1. De verwerking geschiedt slechts voor de volgende doelen:
   a. de beoordeling van de geschiktheid van betrokkene voor een functie die vacant is of kan komen;
   b. de afhandeling van de door de sollicitant gemaakte onkosten;
   c. de interne controle en de bedrijfsbeveiliging;
   d. de uitvoering of toepassing van een andere wet.

2. Geen andere gegevens worden verwerkt dan:
   a. de in bijlage 1 onder a, b en c genoemde gegevens;
   b. een administratienummer dat geen andere informatie bevat dan bedoeld onder a;
   c. gegevens betreffende gevolgde en te volgen opleidingen, cursussen en stages;
   d. gegevens betreffende de functie waarnaar gesolliciteerd is;
   e. gegevens betreffende de aard en inhoud van de huidige dienstbetrekking, alsmede betreffende de beëindiging ervan;
   f. gegevens betreffende de aard en inhoud van de vorige dienstbetrekkingen, alsmede betreffende de beëindiging ervan;
   g. andere gegevens met het oog op het vervullen van de functie, die door de betrokkene zijn verstrekt of die hem bekend zijn;
   h. andere dan de onder a tot en met g bedoelde gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van geldende wet- en regelgeving.

Privacyreglement CSG Jan Arentsz

Bijlage 3: Administratie personeel, salaris, uitdiensttreding en pensioen

1. De verwerking geschiedt slechts voor de volgende doelen:
   a. het geven van leiding aan de werkzaamheden van betrokkene;
   b. de behandeling van personeelszaken;
   c. het berekenen, vastleggen en betalen van salarissen, vergoedingen en andere geldsommen en beloningen in natura aan of ten behoeve van betrokkene;
   d. het regelen van aanspraken op uitkeringen in verband met de beëindiging van een dienstverband, waaronder de berekening, de vastlegging en de betaling van deze uitkeringen aan of ten behoeve van de betrokkenen;
   e. het berekenen, vastleggen en betalen van belasting en premies ten behoeve van betrokkene;
   f. het vastleggen van een voor de betrokkene geldende arbeidsvoorwaarde;
   g. de opleiding van betrokkene;
   h. de bedrijfsmedische zorg voor betrokkene;
   i. het bedrijfsmaatschappelijk werk;
   j. de verkiezing van de leden van een bij wet geregeld medezeggenschapsorgaan;
   k. de interne controle en de bedrijfsbeveiliging;
   l. de uitvoering van een voor de betrokkene geldende arbeidsvoorwaarde;
   m. het opstellen van een lijst van data van verjaardagen van betrokkenen en andere feestelijkheden en gebeurtenissen;
   n. het verlenen van ontslag;
   o. het innen van vorderingen, waaronder begrepen het in handen van derden stellen van die vorderingen;
   p. het behandelen van geschillen en het doen uitoefenen van accountantscontrole;
   q. andere dan de onder a tot en met q bedoelde gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van geldende wet- en regelgeving.

2. Geen andere persoonsgegevens worden verwerkt dan:
   a. de in bijlage 1 onder a, b en c genoemde gegevens;
   b. een administratienummer dat geen andere informatie bevat dan bedoeld onder a;
   c. gegevens betreffende gevolgde en te volgen opleidingen, cursussen en stages;
   d. gegevens betreffende de functie of de voormalige functie, alsmede betreffende de aard, de inhoud en de beëindiging van het dienstverband;
   e. gegevens met het oog op de administratie van de aanwezigheid van de betrokkenen op de plaats waar de arbeid wordt verricht en hun afwezigheid in verband met verlof, arbeidsduurverkorting, bevalling of ziekte, met uitzondering van gegevens over de aard van de ziekte;
   f. gegevens met het oog op het berekenen, vastleggen en betalen van salarissen, vergoedingen en andere geldsommen en beloningen in natura aan of ten behoeve van de in het eerste lid bedoelde personen;
   g. gegevens met het oog op het berekenen, vastleggen en betalen van belasting en premies ten behoeve van betrokkene
   h. gegevens, waaronder begrepen gegevens betreffende gezinsleden en voormalige gezinsleden van de betrokkenen, die noodzakelijk zijn met het oog op een overeengekomen arbeidsvoorwaarde;
   i. gegevens die in het belang van de betrokkenen worden opgenomen met het oog op hun arbeidsomstandigheden;

j. gegevens met oog op het organiseren van de personeelsbeoordeling en de loopbaanbegeleiding, voor zover die gegevens bij de betrokkenen bekend zijn;
k. andere dan de onder a tot en met k bedoelde gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van een andere wet.

Bevoegdheden Magister
Een gedetailleerd overzicht van de bevoegdheden op naam functionaris is op verzoek in te zien bij de applicatiebeheerder bij de leerlingadministratie.

	docent	mentor	schoolleider	decaan	zorg coördinator	Hoofd congierge	administratie	veiligheids coördinator
leerlingen vak	x							
leerlingen mentorklas		x						
leerlingen onder team			x					
Leerlingen andere vestiging				x	x			
Leerlingen alle vestigingen			x			x	x	x

Bevoegdheden Afas
Een gedetailleerd overzicht van de bevoegdheden op naam functionaris is op verzoek in te zien bij de applicatiebeheerder Afas.

	personeel team / stafafdeling	personeel vestiging	alle personeel	oud-personeel	sollicitanten
Schoolleider/ hoofd stafafdeling	x				
vestigingsdirecteur	x	x			
voorzitter CvB	x	x	x		

Coördinator Oplis	x	x	x		
Medewerker P&O	x	x	x	x	x
Medewerker financiële administratie	x	x	x	x	x
Controller	x	x	x	x	x
Applicatiebeheerder	x	x	x	x	
Leden sollicitatiecommissie					x

16. Wat als je een zwakke plek vindt in een van onze systemen?

Bij Csg Jan Arentsz vinden wij de veiligheid van onze informatiesystemen (internet en bijbehorende hardware en software) erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek (kwetsbaarheid) is. Als jij een zwakke plek in één van onze systemen hebt gevonden, dan horen wij dit graag, zodat we zo snel mogelijk maatregelen kunnen treffen. Wij willen graag met jou samenwerken om de leerlingen, medewerkers en de informatie in onze systemen beter te kunnen beschermen.

Wij vragen jou:

- Je bevindingen te mailen naar Veiligheid@ja.nl of deze te melden bij de helpdesk bij ICT- en Onderwijsondersteuning;
- De kwetsbaarheid niet te misbruiken door bijvoorbeeld meer informatie te downloaden dan nodig is om het lek aan te tonen of informatie van leerlingen, docenten of andere medewerkers in te kijken, te delen, te verwijderen of aan te passen;
- De kwetsbaarheid niet met anderen te delen totdat deze is verholpen en alle informatie die verkregen is via het lek direct na het melden (en indien nodig overdragen van de informatie) van het lek te wissen;
- Geen gebruik te maken van aanvallen op de beveiliging en de internetvoorziening van de school;
- De veiligheidscoördinator/helpdesk van Csg Jan Arentsz voldoende informatie te geven om het probleem te kunnen vinden zodat wij het zo snel mogelijk kunnen verhelpen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij meer ingewikkelde kwetsbaarheden kan extra informatie nodig zijn.

Wij beloven dat:

- Je binnen 3 werkdagen van ons te horen krijgt dat (en zo mogelijk hoe) we de kwetsbaarheid gaan oppakken;
- Wij je op de hoogte houden van de voortgang van het verhelpen van de kwetsbaarheid;
- Als je de kwetsbaarheid direct na constateren gemeld hebt en via de bovenstaande stappen gehandeld hebt, wij tegen jou geen melding/aangifte zullen doen bij de politie*;
- Jouw melding door ons vertrouwelijk wordt behandeld en dat jouw persoonlijke gegevens niet zonder jouw toestemming met anderen gedeeld worden (tenzij dit wettelijke verplicht is);
- Wij het waarderen wanneer je een kwetsbaarheid meldt en daar een passende beloning tegenoverstellen

* Let op: ons beleid voor het melden van zwakke plekken is geen uitnodiging om ons netwerk uitgebreid te scannen om deze te ontdekken.

Constateer je iets waarvan je vermoedt dat het niet klopt meld dat dan direct bij veiligheid@ja.nl **of de helpdesk.** Zo verklein je in ieder geval de kans dat je tijdens jouw 'zoektocht' onbedoeld handelingen uitvoert die mogelijk strafbaar zijn.

Cc/by/3.0 NL

Geschreven door Floor Terra (responsibledisclosure.nl), bewerkt door Kennisnet en Csg Jan Arentsz.