

Informatiebeveiliging en privacy beleid Stichting Keizer Karel

Vastgesteld GMR d.d. 3 december 2018

Inleiding

Het onderwijs is in toenemende mate afhankelijk van informatie en Informatie verwerkende systemen (verder te noemen ICT). De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door het gebruik van digitale leermiddelen. 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.

1. Informatiebeveiliging en privacy

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 imagooverlies.

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 (bewaren, opslaan, bewerken, vernietigen etc.).

Informatiebeveiliging en privacy (IBP)

Informatiebeveiliging is een belangrijke voorwaarde 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 beleid: IBP. Dit beleid vormt de basis om informatiebeveiliging en privacy binnen de Stichting Keizer Karel te regelen en vormt de kapstok voor de onderliggende afspraken en procedures, welke in de bijlage benoemd zijn.

2. Doel en reikwijdte

Doel

Informatiebeveiliging en privacy heeft de volgende doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering binnen de Stichting Keizer Karel en het daaraan verbonden Alkwin Kollege en het Keizer Karel College.
- Het garanderen van de privacy van alle betrokkenen waarvan de Stichting Keizer Karel 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 de Stichting Keizer Karel voldoet aan relevante wet- en regelgeving.

Reikwijdte

- Het IBP-beleid binnen stichting Keizer Karel geldt voor alle medewerkers, leerlingen, ouders/verzorgers, stagiaires, vrijwilligers, sollicitanten, (geregistreeerde) bezoekers en externe relaties (inhuur / outsourcing) van de stichting en/of het daaraan verbonden Alkwin Kollege of Keizer Karel College. Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot de schoolnetwerken verkregen kan worden.
- Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Stichting Keizer Karel en/of het daaraan verbonden Alkwin Kollege of Keizer Karel College, waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, stagiaires, vrijwilligers, sollicitanten, (geregistreeerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan de stichting persoonsgegevens verwerkt.
- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van Stichting Keizer Karel. 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 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 de Stichting Keizer Karel 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 de Stichting Keizer Karel raakvlakken met:
 - *Algemeen veiligheids- en toegangsbeveiligingsbeleid*; met als aandachtspunten het schoolveiligheidsplan, het camera protocol, het medisch protocol, 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.

3. Uitgangspunten

De Stichting Keizer Karel hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het schoolbestuur van de Stichting Keizer Karel 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. De Stichting Keizer Karel voldoet aan alle relevante wet- en regelgeving.
3. Bij de Stichting Keizer Karel 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 de stichting 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 te allen tijde hun toestemming herzien.
4. De Stichting Keizer Karel 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. De Stichting Keizer Karel legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. De Stichting Keizer Karel voldoet hiermee aan de documentatieplicht.
6. Binnen de Stichting Keizer Karel 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. De Stichting Keizer Karel 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. De Stichting Keizer Karel 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. De Stichting Keizer Karel 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. De Stichting Keizer Karel verwacht van alle medewerkers, leerlingen, **ouders/verzorgers**, stagiaires, vrijwilligers, sollicitanten, (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 imagooverlies. De Stichting Keizer Karel heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.

11. Informatiebeveiliging en privacy is bij de Stichting Keizer Karel een continu proces, waarbij jaarlijks wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
12. De Stichting Keizer Karel 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. De Stichting Keizer Karel neemt passende organisatorische en/of 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. Daar waar het beheer van de ICT infrastructuur extern belegd is worden aanvullende afspraken gemaakt over de technische maatregelen.
14. De Stichting Keizer Karel zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

4. Uitvoering van het IBP beleid

Dit hoofdstuk beschrijft de uitvoering van het IBP beleid binnen de Stichting keizer Karel.

Relevante wet- en regelgeving

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

- Wet op het voortgezet onderwijs
- Wet goed onderwijs en goed bestuur VO
- Wet onderwijstoezicht
- Algemene Verordening Gegevensbescherming (AVG)
- 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.

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:

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.
2. **Grondslag:** verwerking van persoonsgegevens is gebaseerd op een van de zes wettelijke grondslagen.
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 (subsidiar). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.
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.
5. **Data-integriteit:** er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

Ondersteunende richtlijnen en procedures

Diverse aanvullende reglementen, procedures en protocollen geven invulling aan de uitwerking van het IBP beleid. De uitwerking van het beleid kan verschillen voor de aan de Stichting Keizer Karel verbonden scholen (Alkwin Kollege of Keizer Karel College). In de bijlage een overzicht van de diverse aanvullende reglementen, procedures en protocollen. De verwerkingen van persoonsgegevens worden op stichtingsniveau vastgelegd en up-to-date gehouden in het 'Dataregister verwerkingen'.

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 het hoofd ICT, het hoofd bedrijfsvoering, de school- en afdelingsleiding, de rector en het bestuur als eindverantwoordelijke.

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.

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 het 'Meldpunt datalekken'. Deze is ondergebracht bij de afdeling ICT.

Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden. Datalekken worden gemeld bij de Autoriteit Persoonsgegevens.

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;
- de actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving, etc.

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 leidinggevend en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP in diverse publicaties, thema lessen (mediawijsheid) en 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 door de Stichting Keizer Karel extern ingehuurd en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak.

Mocht naleving van dit beleid ernstig tekort schieten, dan kan de Stichting Keizer Karel de betrokken verantwoordelijke medewerkers een sanctie op leggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

Logging en monitoring

Logging en monitoring door de afdeling ICT 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.

Bijlage 1

Het IBP-beleid van de stichting Keizer Karel vormt de basis om informatiebeveiliging en privacy binnen de Stichting Keizer Karel te regelen en dient als de kapstok voor de onderliggende afspraken en procedures.

- Privacy Reglement
- Protocol datalekken
- Gedragscode ICT en internetgebruik
- Protocol sociale media
- Protocol gebruik beeldmateriaal
- Protocol cameratoezicht
- Register verwerkingen, inclusief classificatie
- Overzicht verwerkersovereenkomsten