Informatiebeveiligings- en privacy beleid
Lyceum Sancta Maria

Inhoudsopgave

1 Inleiding

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. 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.

2 Toelichting informatiebeveiliging en privacy

2.1 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. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

2.2 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.

2.3 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 de Stichting R.K. Scholengemeenschap Sancta Maria (hierna te noemen: Sancta Maria) te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

3 Doel en reikwijdte

3.1 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 Sancta Maria 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 Sancta Maria voldoet aan relevante wet- en regelgeving.

3.2 Reikwijdte

- Het IBP-beleid binnen Sancta Maria 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 Sancta Maria waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan Sancta Maria persoonsgegevens verwerkt.

- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van Sancta Maria.

- Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van Sancta Maria 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 Sancta Maria o.a. 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.
  - *ICT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ICT.
  - *Medezeggenschap* van leerlingen, hun ouders/verzorgers en medewerkers.
  - *Professionaliseringsbeleid* met als aandachtspunt de digitaal-didactische vaardigheden en mediawijsheid onderwijzend personeel.
  - *Onderwijsbeleid-met als aandachtspunten:*
    - Beleid inzake aanschaf en gebruik van digitale leeromgeving, digitale leermiddelen
    - Toets- en examenbeleid, voorkomen van fraude.
    - Doorstroomgegevens uitwisselen met basisscholen en vervolgonderwijs.

4 Beleid – uitgangspunten

Sancta Maria hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het dagelijks bestuur van Sancta Maria neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. Zij is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het dagelijks bestuur de verwerkingsverantwoordelijke. Het toezichthoudend deel van het bestuur heeft een toezichthoudende rol.

2. Sancta Maria voldoet aan alle relevante wet- en regelgeving.

3. Bij Sancta Maria 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 Sancta Maria 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. Sancta Maria zal alle betrokkenen helder en actief informeren over de verwerkingen van 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. Sancta Maria legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. Sancta Maria voldoet hiermee aan de documentatieplicht.

6. Binnen Sancta Maria 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. Sancta Maria is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt gebruikt.

8. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen en de tenemen maatregelen.

9. Sancta Maria maakt met partijen waarmee persoonsgegevens worden uitgewisseld concrete afspraken over de informatiebeveiliging en privacy (middels een verwerkingsovereenkomst).

10. Informatiebeveiliging en privacy is bij Sancta Maria een continu proces, waarbij regelmatig (minimaal jaarlijks) processen worden geëvalueerd en wordt gekeken of aanpassing gewenst is.

11. Sancta Maria 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.

12. Sancta Maria 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.

13. Sancta Maria zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en zo nodig melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

4.1 Relevante wet- en regelgeving

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

- Wet voortgezet onderwijs en/of Wet op de expertisecentra
- Wet goed onderwijs en goed bestuur VO
- Wet onderwijstoezicht
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht
- CAO VO
- Wet Passend Onderwijs
- Examens en toetsing (gepubliceerd op Examenblad.nl)

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.

4.2 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: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokke of gerechtvaardigd belang.

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.

5 Uitwerking van het beleid- Wat doen we?

5.1 Ondersteunende richtlijnen en procedures

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het IBP-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.

5.2 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. Binnen teams is een privacytegel opgenomen waaronder alle actuele documenten geplaatst zijn. Daarnaast wordt er periodiek informatie via Sanctamemo verspreid en is er een privacy-boekje met praktische informatie speciaal voor medewerkers.

5.3 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.

5.4 Incidenten en datalekken

Alle mogelijke (beveiligings-)incidenten worden gemeld bij privacy@sanctamaria.nl. Alle medewerkers, die een beveiligingsincident of datalek vermoeden dienen dit te melden. In het protocol 'informatiebeveiligingsincidenten en datalekken', is de procedure van afhandeling vastgelegd. 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. Periodiek zullen de beveiligingsincidenten besproken worden met de schoolleiding en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

5.5 Planning en controle

Dit IBP-beleid wordt minimaal elk jaar getoetst en zo nodig bijgesteld. Hierbij wordt rekening gehouden met:

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

Daarnaast maakt Sancta Maria jaarlijks een IBP-jaarplanning waarin de planning en control cyclus voor informatiebeveiliging en privacy is opgenomen. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst.

5.6 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 hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen.

Voor toezicht op de naleving van de AVG heeft Sancta Maria een externe Functionaris Gegevensbescherming. De externe Functionaris gegevensbescherming heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. Sancta Maria heeft daarnaast een privacy officer. Deze medewerker is o.a. verantwoordelijk voor het ontwikkelen, bewaken en toetsen van het privacybeleid. Tevens biedt de privacy officer ondersteuning bij de uitvoering van dit beleid, is het eerste aanspreekpunt voor alle betrokkenen (intern en extern) en geeft gevraagd en ongevraagd advies over privacy gerelateerde onderwerpen.

De privacy officer is Susanne de Wit en is te bereiken via
privacy@sanctamaria.nl

5.7 Logging en monitoring

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

6 Organisatie - Wie doet wat?

6.1 Rollen en verantwoordelijkheden

Het dagelijks bestuur
Het dagelijks bestuur is eindverantwoordelijk voor het IBP-beleid en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast. Het toezicht houdende deel van het bestuur heeft een toezichthoudende rol.

De Externe Functionaris Gegevensbescherming
De externe functionaris gegevensbescherming houdt toezicht op de toepassing en naleving van de AVG. De wettelijke taken en bevoegdheden geven deze functionaris een onafhankelijke positie.

De privacy officer
Sancta Maria heeft een privacy officer aangesteld.
Taken van de interne functionaris gegevensbescherming:

- is eerste aanspreekpunt en vraagbaak op het gebied van informatiebeveiliging en privacy beleid (IBP-beleid) voor de gehele organisatie en externen;
- adviseert bij de ontwikkeling van het IBP-beleid;
- vertaalt IBP-beleid naar richtlijnen, procedures, maatregelen en documenten voor de gehele organisatie en houdt deze up-to-date;
- voert, op verzoek van het bestuur, interne audits uit ter controle en verbetering van bestaande processen;
- controleert verwerkingsovereenkomsten en houdt het verwerkingsregister bij;
- is het aanspreekpunt voor incidenten op het gebied van informatiebeveiliging en privacy;
- stelt een IBP-jaarplanning op en maakt een jaarverslag;
- handelt incidenten op het gebied van informatiebeveiliging en privacy af;
- adviseert en ondersteund dagelijks bestuur, afdelingsleiders en medewerkers bij de implementatie IBP-beleid of IBP-vraagstukken;
- handelt aanvragen betreffende informatie, inzage, verbetering, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit en profilering van betrokkenen af.
- beheert de archiefkamer en zorgt dat het papierarchief dat hier is opgeslagen voldoet aan onder andere de archiefwet;
- is contactpersoon voor en werkt samen met de externe functionaris gegevensbescherming.

Afdeling ICT
De werkzaamheden van de afdeling ICT bestrijken een breed gebied van ICT in onderwijs en bedrijfsvoering; informatiebeveiliging en privacy is één van de aandachtspunten. De afdeling ICT adviseert het dagelijks bestuur en het MT en ziet toe op naleving van het IBP-beleid in de primaire ICT-processen van Sancta Maria in nauwe samenwerking met de interne functionaris gegevensbescherming.

Schoolleiding (SL) en Teamleiders (TL)
Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft op uitvoerend niveau de taak om:

- ervoor te zorgen dat de medewerkers op de hoogte zijn van het IBP-beleid;
- toe te zien op de naleving van het IBP-beleid door de medewerkers, waarbij de leidinggevende zelf een voorbeeldfunctie heeft;
- periodiek het onderwerp IBP onder de aandacht te brengen in werkoverleggen, beoordelingen etc

Medewerker
Elke medewerker heeft verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in zijn of haar dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn o.a. beschreven in de ‘beleid ICT-bedrijfsmiddelen’. Medewerkers wordt gevraagd om actief betrokken te zijn bij informatiebeveiliging en het privacybeleid. Medewerkers maken melding van datalekken en beveiligingsincidenten en kunnen verbetervoorstellen doen

Bijlage 1: Ondersteunende richtlijnen en procedures

Nr.	Document	Actuele versie	Openbaar/ waar plaatsen
1	Sancta IBP-beleid	November 2022	Websit en teams/ informatieboekje
2	Sancta Privacyreglement	November 2022	Website en Teams/informatieboekje
3	Privacyverklaring leerlingen en ouders	November 2022	Website
4	Privacyverklaring medewerkers	November 2022	Teams
5	Privacyverklaring sollicitanten	November 2022	Website
6	Protocol ICT	November 2022	Teams/ informagieboekje
7	Responsible disclosure Leerlingen en externen	November 2022	Website
8	Responsible disclosure medewerkers	November 2022	Website en Teams
9	Protocol datalekken en beveiligingsincidenten	November 2022	Website en Teams/ informatieboekje
10	Protocol gebruik camera en videobeelden	November 2022	Website en Teams/informatieboekje
11	Protocol bewaartermijnen en verwijdering gegevens	November 2022	Teams/informatieboekje
12	Uitwerking bewaartermijnen	November 2022	Teams
13	IBP jaarplanning 2022-2023	November 2022	Intern document