

Informatiebeveiligings- en privacy beleid

Emelwerda College

Bron

saMBO-ICT
Kennisnet

Bewerkt door:

Emelwerda College

Versie	Status	Bijgewerkt d.d. datum	Auteur	Omschrijving
		20-nov-20	Hie	Informatiebeveiligings- en privacy beleid

**Vastgesteld door de directie en de Raad van Bestuur van het
Emelwerda College**

te Emmeloord

Versie	Datum	Naam	Functie
	20-nov-20	A.Leijenaar	Rector Bestuurder

1	INLEIDING	3
	INFORMATIEBEVEILIGING EN PRIVACY	3
2	DOEL EN REIKWIJDTE	3
3	UITGANGSPUNTEN	4
	PRIVACY	4
4	ORGANISATIE	5
	RICHTINGGEVEND	5
	STUREND.....	5
	UITVOEREND.....	5
5	CONTROLE EN RAPPORTAGE	6
	VOORLICHTING EN BEWUSTZIJN.....	6
	CLASSIFICATIE EN RISICOANALYSE.....	6
	INCIDENTEN EN DATALEKKEN	7
	CONTROLE, NALEVING EN SANCTIES	7
	BIJLAGE 1: TABEL IBP ROLLEN EN TAKEN	8

1 Inleiding

Informatie en ict zijn noodzakelijk in de ondersteuning van het onderwijs. Omdat we met persoonsgegevens (van onszelf, leerlingen en anderen) werken, is privacywetgeving daarop van toepassing.

De informatie en ict van Emelwerda College worden blootgesteld aan een groot aantal bedreigingen, al dan niet opzettelijk van aard. Alle informatie die we bewaren en verwerken kan worden bedreigd door een aanval, een vergissing, de natuur (bijv. overstroming of brand). Het niet beschikbaar zijn van ict, incorrecte administraties en het uitlekken van gegevens tot inbreuken op het geven van onderwijs en het vertrouwen in onze school.

Deze bedreigingen maken het noodzakelijk om gerichte maatregelen te treffen om de risico's die gepaard gaan met deze bedreigingen tot een aanvaardbaar niveau te reduceren. Om dit structureel op te pakken is het noodzakelijk dat we een duidelijk maken waar het om gaat, een doel stellen en de manier waarop we dit doel willen bereiken.

Informatiebeveiliging en privacy

Informatiebeveiliging is een proces voor het beschermen van Emelwerda College tegen risico's en bedreigingen met betrekking tot informatie en ict. Het richt zicht op drie aspecten:

- Beschikbaarheid; informatie en aanverwante bedrijfsmiddelen zijn toegankelijk wanneer nodig;
- Integriteit; informatie en verwerkingsmethoden bevatten zo min mogelijk fouten;
- Vertrouwelijkheid; informatie is alleen toegankelijk voor diegenen die daartoe bevoegd zijn.

Privacy gaat om de bescherming van persoonsgegevens conform de huidige AVG wet- en regelgeving. Door het goed toepassen van informatiebeveiliging kan aan deze wetgeving worden voldaan. Vooral het aspect vertrouwelijkheid is hiervoor van belang. Informatiebeveiliging is daarom integraal onderdeel van privacy.

Om privacy goed te regelen is informatiebeveiliging nodig. Daarom zien we het als één onderwerp: informatiebeveiliging en privacy (IBP).

2 Doel en reikwijdte

Dit beleid heeft als doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van leerlingen en medewerkers waardoor beveiligings- en privacy-incidenten en de eventuele gevolgen hiervan worden voorkomen.

Dit beleid is een leidraad voor iedereen die betrokken is bij IBP binnen Emelwerda College. Het is van toepassing op onze eigen medewerkers, tijdelijk personeel en andere personen die een rol spelen in Emelwerda College. Het is van toepassing op de hele organisatie van Emelwerda College, waaronder de fysieke locaties, systemen op interne en externe locaties en gegevensverzamelingen die gebruikt worden.

Het informatiebeveiligings- en privacybeleid heeft raakvlak met andere beleidsgebieden, te weten:

- Algemeen veiligheids- en beveiligingsbeleid; met als aandachtsgebieden bedrijfshulpverlening, fysieke toegang en -beveiliging, crisismanagement, huisvesting en ongevallen;
- IT-beleid; met als aandachtsgebieden de aanschaf en het beheer van ict;
- Personeels- en organisatiebeleid; met als aandachtsgebieden in- en uitstroom van medewerkers, functiescheiding en vertrouwensfuncties;

Dit beleid maakt duidelijk waar de verantwoordelijkheden rondom informatiebeveiliging en privacy zijn belegd.

3 Uitgangspunten

De belangrijkste beleidsuitgangspunten bij het Emelwerda College zijn:

- Informatiebeveiliging en het privacy dient te voldoen aan alle relevante wet- en regelgeving
- Veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen
- Er wordt van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties verwacht dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid
- Het Emelwerda College is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt gebruikt
- Het Emelwerda College maakt met alle partijen waarmee persoonsgegevens worden uitgewisseld concrete afspraken over informatiebeveiliging en privacy
- IBP is een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is
- Er is een balans tussen de risico's van hetgeen we willen beschermen en de benodigde investeringen en maatregelen
- Er is een balans tussen privacy, functionaliteit/werkbaarheid en veiligheid

Privacy

Het Emelwerda College hanteert de vijf vuistregels voor privacy:

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 wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag:** verwerking van Persoonsgegevens is gebaseerd op een van de wettelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene, 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. 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 deze betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun Persoonsgegevens. Daarnaast 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.

Doelgroep zijn de personen wiens gegevens verzameld, verwerkt en gebruikt worden

De betrokkenen hebben er belang bij dat hun data tegen misbruik zijn beschermd. Als gevolg van de AVG krijgen zij bepaalde rechten. Rechten op informatie over, op verandering van of zelfs verwijdering van data. Instellingen hebben een informatieplicht richting de betrokken personen.

Dataminimalisatie in relatie tot gebruik

Persoonsgegevens mogen alleen worden verzameld en verwerkt als daarvoor een grondige reden bestaat en als daarvoor toestemming is gegeven. Voorkomen moet worden dat data verzameld wordt, die niet strikt noodzakelijk zijn, ook vanwege de daaraan gekoppelde inspanningen.

Hierbij gelden de volgende principes (Artikel 25 in de AVG):

- Privacy-by-design (Gegevensbescherming door ontwerp)
- Privacy-by-default (Gegevens bescherming door standaardinstellingen)

Wet- en regelgeving

Het Emelwerda College voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs
- Wet goed onderwijs en goed bestuur PO/VO
- Wet bescherming persoonsgegevens

- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

Hiernaast zijn de bepalingen van het convenant 'Digitale onderwijsmiddelen en privacy 2.0' leidend bij het maken van afspraken met leveranciers.

4 Organisatie

Dit hoofdstuk beschrijft hoe IBP in het Emelwerda College is georganiseerd. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

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

Voor elk niveau wordt beschreven welke rollen welke verantwoordelijkheden en taken hebben en wat de documenten zijn die daarbij passen.

Richtinggevend

Eindverantwoordelijke

De Raad van Bestuur/directie is eindverantwoordelijk voor IBP en stelt het beleid en de maatregelen vast op het gebied van informatiebeveiliging en privacy. De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages door hen geëvalueerd. Binnen het CvB/de RvB/de directie is het hoofd ICT verantwoordelijk voor IBP.

Sturend

Hoofd IBP

Hoofd IBP is een rol op sturend niveau. Deze geeft terugkoppeling en advies geeft aan de eindverantwoordelijke en stuurt de mensen aan op de uitvoerende laag. Het hoofd IBP moet:

- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling
- De uniformiteit bewaken binnen het Emelwerda College
- Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy
- De verdere afhandeling van incidenten binnen het Emelwerda College coördineren

Domeinverantwoordelijkheid/proceseigenaar

Binnen de school zijn er verschillende domeinen/processen, zoals ict, personeel, administratie 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.

Leidinggevend hebben een voorbeeldrol ten opzichte van hun medewerkers.

Uitvoerend

Functionaris voor Gegevensbescherming

De functionaris voor gegevensbescherming (FG) houdt binnen het Emelwerda College toezicht op de toepassing en naleving van de privacy-wetgeving. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie.

De FG heeft bij voorkeur een externe aanstelling en wordt op basis van een contract ingehuurd.

De FG zorgt voor het afhandelen van vertrouwelijke informatiebeveiligingsincidenten.

De FG heeft overleg met manager IBP en de Privacy Officer .

De FG kan ook contactpersoon zijn voor klachten en vragen van betrokkenen met een vertrouwelijk karakter.

De Privacy Officer voor gegevensbescherming

De PO heeft de volgende taken en verantwoordelijkheden:

- Informeren en adviseren van de directie
- Controleren (op de naleving van de AVG)
- Adviseren op aanvraag
- Samenwerken met de autoriteiten

Veel zaken die in de praktijk als haalplicht van de Data Protection Officer worden beschouwd, worden in de wetgeving juist als brengplicht aangemerkt. De directie of de betrokken afdelingen moeten daarvoor zorgen. Zij dienen verantwoord met persoonsgegevens om te gaan.

Medewerker

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in het personeelshandboek en de handleiding aanvaardbaar gebruik van bedrijfsmiddelen. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.

Medewerkers worden andere 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 OR)

Leidinggevende

Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering.

Iedere leidinggevende heeft op uitvoerend niveau de taak om:

- er voor te zorgen dat zijn medewerkers op de hoogte zijn van het beveiligingsbeleid;
- toe te zien op de naleving van het IBP-beleid door de medewerkers, waarbij hij/zij zelf een voorbeeld-functie 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, de FG en de Privacy Officer..

5 Controle en rapportage

Dit informatiebeveiligings- en privacybeleid wordt minimaal elke twee jaar getoetst en bijgesteld door het MT. Hierbij wordt rekening gehouden met:

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

Daarnaast kent het Emelwerda College een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst.

Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt bij het Emelwerda College 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, deelnemers en gasten. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van de manager IBP / informatie manager/ Security Officer met het College van Bestuur als eindverantwoordelijke.

Classificatie en risicoanalyse

Bij het Emelwerda College heeft alle informatie waarde, daarom worden alle gegevens waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de 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 kwaliteitsaspecten die van belang voor de informatievoorziening.

Incidenten en datalekken

Alle incidenten kunnen worden gemeld bij de directleidinggevende / hoofd ICT [/helpdesk@emelwerda.nl](mailto:helpdesk@emelwerda.nl)
De afhandeling van deze incidenten volgt een gestructureerd proces, die ook voorziet in de juiste stappen rondom de meldplicht datalekken.

Controle, naleving en sancties

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het IBP proces. Van belang hierbij is dat leidinggevend en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Bij het Emelwerda College wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode, met periodieke bewustwordingscampagnes, et cetera.

Voor de bevordering van de naleving van de Wet bescherming persoonsgegevens vervult de Functionaris Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door de Raad van Bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het RvB vast te stellen reglement.

Mocht de naleving ernstig tekort schieten, dan kan het Emelwerda College de betrokken verantwoordelijke medewerkers een sanctie op leggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

Bij het Emelwerda College is het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol.

Bijlage 1: Tabel IBP rollen en taken

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richtinggevend (strategisch)	Voorbeelden: Bestuur CvB Directeur	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Informatiebeveiligings- en privacy beleid Baseline / basismaatregelen Reglement FG vaststellen Privacyreglement vaststellen
Sturend (tactisch)	Hoofd ICT / IBP	<ul style="list-style-type: none"> 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 procedures om de uitvoering te ondersteunen 	<p>Processen, richtlijnen en procedures IBP, waaronder:</p> <ul style="list-style-type: none"> activiteitenkalender Protocol beveiligingsincidenten en datalekken Bewerkersovereenkomsten regelen Brief toestemming gebruik foto's en video Opstellen informatie documentatie richting leerlingen, ouders / verzorgers Security awareness activiteiten Sociale media reglement Gedragscode ict en internetgebruik Gedragscode medewerkers en leerlingen
	Functionaris voor Gegevensbescherming	<ul style="list-style-type: none"> Toezicht op naleving privacy wetgeving Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens Afwikkeling klachten en incidenten 	<ul style="list-style-type: none"> Privacyreglement, procedure IBP-incident afhandeling Inrichten meldpunt datalekken
	Domeinverantwoordelijke/ Proceseigenaren waaronder: ict, personeel (HRM / P&O), Facilitair, onderwijs, financiën, inkoop en administratie	<ul style="list-style-type: none"> Classificatie / risicoanalyse in samenwerking met Manager IBP (Informatie-manager / verantwoordelijke IBP / Security officer) Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door <i>bestuur/CvB/directie</i> <i>Samen met functioneel beheer en ICT beheer</i> er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. <i>Samen met functioneel beheer en ICT beheer</i> de toegangsrechten van gebruikers regelmatig beoordelen en controleren. 	<ul style="list-style-type: none"> Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst) Classificatie- en risicoanalyse documenten. <p>Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder:</p> <ul style="list-style-type: none"> Toegangsmatrix diverse informatiesystemen en netwerk

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen Vanuit de Wiki
Uitvoerend (operationeel)	Privacy officer Medewerker Dagelijkse leiding / leidinggevende / directie	<ul style="list-style-type: none"> • Incidentafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor IBP-incidenten. • Uitvoeren taken conform gegeven richtlijnen en procedures. • Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden. • 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. 	Communiceren, informeren en toezien op naleving van o.a.: <ul style="list-style-type: none"> • IBP in het algemeen • Regels passend onderwijs • Hoe om te gaan met leerling dossiers • Wie mogen wat zien • Gedragscode • Omgaan met sociale media • Mediawijs maken