Tobiasschool SBO

Informatiebeveiligings- en privacy beleid (IBP)

Versie: 25 mei 2018

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 de Stichting Tobiasschool 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), etcetera. Het niet beschikbaar zijn van ICT, incorrecte administraties en het uitlekken van gegevens kan leiden tot inbreuken op het onderwijsproces, en het vertrouwen in onze school en onze organisatie in het algemeen.

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 aan te pakken is het noodzakelijk dat we duidelijk maken waar het om gaat, een doel stellen en de manier waarop we dit doel willen bereiken.

1.1. Informatiebeveiliging en privacy

Informatiebeveiliging is een proces om de Stichting Tobiasschool te beschermen 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 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 de Stichting Tobiasschool. Het is van toepassing op onze eigen medewerkers, tijdelijk personeel en andere personen die een rol spelen binnen de Stichting Tobiasschool. Het is van toepassing op de fysieke locatie, 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;
- ICT-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

3.1. Algemene uitgangspunten.

De belangrijkste beleidsuitgangspunten bij de Stichting Tobiasschool 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.
- De Stichting Tobiasschool is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt gebruikt.
- De Stichting Tobiasschool 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.

3.2. Beleidsuitgangspunten Privacy

De Tobiasschool 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.

Persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen.

Bij alle registraties op basis van toestemming, zal de Stichting Tobiasschool aan de betrokkene een eenduidige zogenaamde opt-out procedure worden aangeboden.

4 Wet- en regelgeving

De Stichting Tobiasschool voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet op het primair 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.

5 Organisatie

Dit hoofdstuk beschrijft hoe IBP bij de Stichting Tobiasschool 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.

5.1. Richtinggevend

Eindverantwoordelijke
Het Algemeen Bestuur van de Stichting Tobiasschool 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 jaarlijks geëvalueerd.

5.2. sturend

Sturend Manager IBP
Manager IBP is een rol die weggelegd is voor de directeur/bestuurder op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke en stuurt de mensen aan op de uitvoerende laag. De manager IBP moet:

- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling
- De uniformiteit bewaken binnen de Stichting Tobiasschool (in overleg met de VO afdeling vallend onder VOVA –ROCvA)
- Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy
- De verdere afhandeling van incidenten binnen de Stichting Tobiasschool coördineren

Functionaris voor Gegevensbescherming
De aanstelling van een functionaris voor gegevensbescherming (FG) wordt door het bestuur van de Stichting Tobiasschool aangehouden (besluit mei 2018), i.v.m. de omvang van de school (zie advies (PO/VO raad).

Domeinverantwoordelijkheid/proceseigenaar
Binnen de Stichting Tobiasschool zijn er verschillende domeinen/processen, zoals ICT, personeel, administratie enz. De directeur/bestuurder is verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.

Leidinggevenden hebben een voorbeeldrol ten opzichte van hun medewerkers.

5.3. Uitvoerend

Medewerker
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn o.a. beschreven in het IBP en het privacyreglement Stichting Tobiasschool – leerlingen. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund.

Medewerkers wordt 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.

Leidinggevende
Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering.
De 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 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.

6 Controle en rapportage

Dit informatiebeveiligings- en privacybeleid wordt minimaal een keer per jaar getoetst en bijgesteld door het bestuur van de Stichting Tobiasschool. 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 gaat de Stichting Tobiasschool een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy ontwikkelen.

6.1. 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 de Stichting Tobiasschool 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 directeur/bestuurder met het Bestuur van de Stichting Tobiasschool als eindverantwoordelijke.

6.2. Classificatie en risicoanalyse

Bij de Stichting Tobiasschool 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.

6.3. Incidenten en datalekken

Alle incidenten kunnen worden gemeld bij de directeur/bestuurder. De afhandeling van deze incidenten volgt een gestructureerd proces, die ook voorziet in de juiste stappen rondom de meldplicht datalekken. Zie hiervoor het protocol informatiebeveiligings-incidenten en datalekken van de Stichting Tobiasschool.

6.4. Controle, naleving en sancties

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het IBP proces. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Bij de Stichting Tobiasschool wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met het volgen van een gedragscode, met periodieke bewustwordingscampagnes. Voor de bevordering van de naleving van de Wet bescherming persoonsgegevens vervult de directeur/bestuurder een belangrijke rol.
Mocht de naleving ernstig tekort schieten, dan kan de Stichting Tobiasschool de betrokken verantwoordelijke medewerkers een sanctie op leggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.
Bij de Stichting Tobiasschool is het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol.

Bijlage 1: Tabel IBP rollen en taken

In de praktijk zijn diverse rollen gecombineerd in één persoon.

Niveau	**Wie** **Rollen**	**Hoe** **Verantwoordelijkheid / taken**	**Wat** **Realiseren / vastleggen**
Richtinggevend (strategisch)	Bestuur van de Stichting Tobiasschool	• 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 • basismaatregelen • Privacyreglement vaststellen

Sturend (tactisch)	Directeur/bestuurder	• Inhoudelijk verantwoordelijk voor IBP • IBP-planning en controle • Adviseert bestuur 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	Processen, richtlijnen en procedures IBP, waaronder: • Protocol beveiligingsincidenten en datalekken • activiteitenkalender • Bewerkersovereenkomsten regelen • Brief toestemming gebruik foto's en video • Opstellen informatie documentatie richting leerlingen, ouders / verzorgers • Sociale media reglement • Gedragscode ICT en internetgebruik • Gedragscode medewerkers en leerlingen
	Functionaris voor Gegevensbescherming (niet benoemd) taak naar directeur/bestuurder	• Toezicht op naleving privacy wetgeving • 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
	Proceseigenaren waaronder:	**Classificatie / risicoanalyse** *in samenwerking met Manager IBP (Informatiemanager*	Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst)

	ICT, personeel, materieel, onderwijs, financiën, administratie	• Toegangsbeleid zowel fysiek als digitaal vaststellen • *Samen met functioneel beheer en ICT beheer* (uitbesteed aan de VOVA)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* (uitbesteed aan de VOVA) beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren.	• Classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen Vanuit de Wiki
Uitvoerend (operationeel)	Directeur/ bestuurder Medewerker Dagelijkse leiding / leidinggevende / directie	• Incidentafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor IBP-incidenten. • 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	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

		werkoverleggen, beoordelingen etc.; - Rapporteren voortgang m.b.t. doelstellingen IBPbeleid aan bestuur.	