IRIS onderwijs en opvang

Informatiebeveiligings- en privacy beleid

IRIS VCO
IRIS stichting Kindcentra
IRIS stichting Tussenschoolse Opvang
IRIS stichting Steunfonds

Dit informatiebeveiligings- en privacybeleid is gebaseerd op het standaard beleid dat ontwikkelt is door Verus / Kennisnet. Daar waar nodig is het IRIS-specifiek gemaakt.

Bewerkt door:
IRIS onderwijs en opvang, Gerard Wolters

Versie	Status	Datum	Auteur	Omschrijving
1.0	Concept	19-4-2018	G. Wolters	
1.1	Concept	30 mei 2018	G. Wolters	IRIS Steunfonds toegevoegd

Vastgesteld door college van bestuur IRIS VCO, IRIS Kindcentra, IRIS TSO en IRIS Steunfonds

Versie	Datum	Naam	Functie
		Friso Kingma	Voorzitter CvB

1. Inleiding

Informatie en ict zijn noodzakelijk in de ondersteuning van het onderwijs en de kindopvang. Omdat we met persoonsgegevens (van onszelf, kinderen en anderen) werken, is privacywetgeving daarop van toepassing. Dit beleid geldt voor zowel schoolorgansiatie IRIS, IRIS Kindcentra, IRIS TSO en IRIS Steunfonds, in het vervolg te noemen IRIS.

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

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 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 voor het beschermen van IRIS tegen risico's en bedreigingen met betrekking tot informatie en ict. Het richt zich 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 IRIS. Het is van toepassing op onze eigen medewerkers, tijdelijk personeel en andere personen die een rol spelen bij IRIS, zoals het onderwijsbureau en ICTonderhouders. Het is van toepassing op de hele organisatie van IRIS, 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 sociale-, psychische- en fysieke beveilging (veiligheidsbeleid IRIS – 2016);
- IT-beleid: met als aandachtsgebieden de aanschaf en het beheer van ict (nog te ontwikkelen, schooljaar 2018-2019);
- Gedragscode IRIS (2014) en HRM-beleid (2016);

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

3. Uitgangspunten

De belangrijkste beleidsuitgangspunten bij IRIS zijn:

- Informatiebeveiliging en het privacybeleid dient te voldoen aan wet- en regelgeving
- Veilig en betrouwbaar omgaan met informatie is 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
- IRIS is eigenaar van de informatie die onder haar verantwoordelijkheid door derden wordt gebruikt
- IRIS maakt met alle partijen waarmee persoonsgegevens worden uitgewisseld concrete afspraken over informatiebeveiliging en privacy, zo mogelijk via overkoepelende organisaties als de PO-raad en de branchevereniging Kinderopvang
- IBP is een continu proces, waarbij regelmatig (minimaal 2-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
- Persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen.
- Bij alle registraties op basis van toestemming, zal IRIS aan de Betrokkene een eenduidige zogenaamde Opt-out procedure worden aangeboden (voorbeeld: als betrokkene op een mailinglist staat, dan moet het voor betrokkene eenvoudig zijn om van deze mailinglist verwijderd te worden).
- Er is een balans tussen privacy, functionaliteit/werkbaarheid en veiligheid

3.1 Vuistregels privacy

IRIS 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 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 (kinderen, 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.

4. Wet- en regelgeving

IRIS voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet Kinderopvang
- Wet Innovatie en Kwaliteit Kinderopvang (IKK)
- Wet op het primair onderwijs
- Code goed onderwijs en goed bestuur PO
- Algemene Verordening Gegevensbescherming (AVG)
- Leerplichtwet

Hiernaast zijn de bepalingen van het convenant 'Digitale onderwijsmiddelen en privacy 3.0' leidend bij het maken van afspraken met leveranciers.

5. Organisatie

Dit hoofdstuk beschrijft hoe IBP binnen IRIS 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 informatie / documentatie is die daarbij past (zie bijlage 1).

5.1 Richtinggevend

Eindverantwoordelijke
Het College van Bestuur 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. Het lid CvB is eerste verantwoordelijk voor IBP.

5.2 Sturend

Manager IBP
Manager IBP is een rol op sturend niveau. Deze 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 IRIS
- Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy
- De verdere afhandeling van incidenten binnen IRIS coördineren

Gezien de relatief kleine staf binnen IRIS zijn de taken van de manager ook belegt bij het lid CvB, die ze desgewenst kan delegeren.

Functionaris voor Gegevensbescherming
De functionaris voor gegevensbescherming (FG) houdt binnen IRIS 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 zorgt voor het afhandelen van vertrouwelijke informatiebeveiligingsincidenten. FG heeft regelmatig overleg met manager IBP. De FG is meestal ook contactpersoon en voor klachten en vragen van betrokkenen met een vertrouwelijk karakter.
IRIS werkt met een externe FG, via de Lumen-groep (www.lumengroup.nl).

Domeinverantwoordelijkheid
Binnen de school is de schooldirecteur verantwoordelijk voor de vertaling van het IBP in de school en het implementeren van de daaruit voortvloeiende richtlijnen, procedures en instructies.Binnen IRIS-opvang ligt deze verantwoordelijkheid bij de manager Kindcentra.

Leidinggevenden hebben een voorbeeldrol ten opzichte van hun medewerkers.

5.3 Uitvoerend

ICT-coördinator
De ICT-coördinator vormt het eerste lijns technisch en functioneel aanspreekpunt voor incidenten en informatiebeveiliging. Zo nodig schakelt de coördinator de ICT-onderhouder (2de lijns), waarmee de school een contract heeft, in.

Medewerker
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven het veiligheidsbeleid IRIS 2016. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund.

Medewerkers worden onder andere gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van beveiligingsincidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (bv. via werkoverleggen)

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 voorbeeldfunctie heeft;
- periodiek het onderwerp IBP onder de aandacht te brengen in werkoverleggen, (functionerings) gesprekken etc.;

- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde IBP-onderwerpen.

De leidinggevende kan in zijn taak ondersteund worden door de manager IBP en/of de FG.

6. Controle en rapportage

Dit informatiebeveiligings- en privacybeleid wordt minimaal elke twee jaar getoetst en bijgesteld door het DO. 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

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 IRIS het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Dit gebeurt ondere andere via werkoverleggen. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van alle leidinggevenden met het College van Bestuur als eindverantwoordelijke.

6.2 Classificatie en risicoanalyse

Bij IRIS 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.
Voorafgaand aan de risico-analyse (schooljaar 2018-2019) vallen binnen IRIS de leerlinggevens (inclusief de leerlingontwikkkelingen) en de personeelsgegevens onder de bepalingen van dit IBP-beleid.

6.3 Incidenten en datalekken

In het Veiligheidsbeleid IRIS (2016) staat omschreven hoe er met dit onderwerp wordt om gegegaan.

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 hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Bij IRIS wordt actief aandacht besteed aan IBP bij de aanstelling/inwerkperode, tijdens (functionerings)gesprekken, met de IRIS-gedragscode (2014), tijdens werkoverleggen et cetera.
Mocht de naleving ernstig tekort schieten, dan kan IRIS de betrokken verantwoordelijke medewerkers een sanctie op leggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

Bijlage 1: Tabel IBP rollen en taken

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richtinggevend (strategisch)	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
Sturend (tactisch)	CvB	• Inhoudelijk verantwoordelijk voor IBP • IBP-planning en controle • Adviseert directie over IBP • Voorbereiden uitvoeren IBP-beleid, Classificatie/risicoanalyse • Hanteren IBP normen en wijze van toetsen • Evalueren IBP-beleid en maatregelen • (Laten) uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze • (Laten) schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen	Processen, richtlijnen en procedures IBP, waaronder: • 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 Gegevens-bescherming / Privacy officer	• 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

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
	Schooldirecteur	• **Classificatie / risicoanalyse** *in samenwerking met Manager IBP (Informatiemanager / verantwoordelijke IBP / Security officer)* • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door *bestuur/CvB/directie* • *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) • Classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk
Uitvoerend (operationeel)	ICT-coördinator Systeem-beheerder	• Incidentafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor IBP-incidenten. • 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.:

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
	Dagelijkse leiding / leidinggevende / directie	• 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.	• IBP in het algemeen • Regels passend onderwijs • Hoe omgaan met leerling dossiers • Wie mogen wat zien • Gedragscode • Omgaan met sociale media • Mediawijs maken