Surplus Alle kansen van de wereld

Privacybeleid

AVG

Contactgegevens Stichting Surplus:
De verwachting 7
1761 VM Anna Paulowna

Verwerkingsverantwoordelijke (bestuurder):
José Vosbergen

Contactgegevens Functionaris Gegevensbescherming (FG):
Wendeline Sjouwerman
FG@stichtingsurplus.nl

Bron
Kennisnet

Bewerkt door:
EFK Interim-management en advies, a.i. privacy officer Sandra Rijkers

Ver-sie	Status	Datum	Auteur	Omschrijving
1.0	Voorlopig vastgesteld	05-06-2019	Kennisnet en bewerkt door Sandra Rijkers	Voorlopig vastgesteld

FG Stichting Surplus:

Versie	Datum	Gevraagd	Besluit/opmerkingen
1.0	05-06-2019	Instemming	instemming

GMR Stichting Surplus:

Versie	Datum	Gevraagd	Besluit/opmerkingen
1.0		Instemming	

CvB Stichting Surplus:

Versie	Datum	Gevraagd	Besluit/Opmerkingen
1.0	05-06-2019	Voorlopige vaststelling	Voorlopig vastgesteld. Na instemming GMR definitief vaststellen.
		Definitief vaststellen	

RvT Stichting Surplus:

Versie	Datum	Gevraagd	Opmerkingen
		Kennisname	

Inhoud

1 Het belang van informatiebeveiliging en privacy

Niet iedereen maakt in zijn leven altijd de juiste keuzes. Normaal gesproken blijven die keuzes privé. Dit geeft ons de gelegenheid om te experimenteren en om fouten te maken waar we van kunnen leren. Een goede bescherming van privacy geeft daarmee de mogelijkheid tot ontwikkeling en groei, zonder geconfronteerd te worden met keuzes of uitlatingen uit het verleden. Leerlingen hebben recht op een veilige (digitale) leeromgeving: een school waar kinderen veilig kunnen experimenteren en fouten kunnen en mogen maken.
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. 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, zoals bijvoorbeeld het uitvallen van systemen en internetcriminaliteit. 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 van de stichting. 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 om informatiebeveiliging en privacy binnen Stichting Surplus 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 Stichting Surplus persoonsgegevens verwerkt, waaronder leerlingen, 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. leerlingen, ouders/verzorgers en medewerkers) wordt gerespecteerd en Stichting Surplus voldoet aan relevante wet- en regelgeving.

3.2 Reikwijdte

- Het IBP-beleid binnen Stichting Surplus geldt voor alle leerlingen, ouders/verzorgers medewerkers, (geregistreerde) bezoekers en externe relaties (zoals bijvoorbeeld inhuur). Onder dit beleid vallen ook alle devices (zowel door de organisatie verstrekte devices als zelf meegebrachte devices) van waar geautoriseerde toegang tot het (school)netwerk verkregen kan worden.
- Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Stichting Surplus waaronder in ieder geval alle leerlingen, ouders/verzorgers medewerkers, (geregistreerde) bezoekers en externe relaties (zoals bijvoorbeeld inhuur), evenals op overige betrokkenen waarvan Stichting Surplus persoonsgegevens verwerkt.
- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van Stichting Surplus. 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 (persoonlijke pagina's van) websites en/of social media.)
- Dit beleid is niet van toepassing op persoonsgegevens opgenomen in bestanden van instanties waarmee de school contact heeft waarbij die instanties als verwerkingsverantwoordelijke gelden (zoals onder andere DUO, UWV of Inspectie van het Onderwijs); in dat geval gelden de privacyregels van de betreffende instantie.
- Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van Stichting Surplus evenals op de daaraan ten grondslag liggende documenten, bijvoorbeeld het aanmeldingsformulier of de akte van benoeming, 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, zoals bijvoorbeeld toestemmingformulieren.
- IBP-beleid heeft binnen Stichting Surplus raakvlakken met:
  - *Personeels- en organisatiebeleid;* met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen en functiescheiding;
  - *IT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ict en (digitale) leermiddelen;
  - *Medezeggenschap* van leerlingen, ouders/verzorgers en medewerkers.

4 Beleid – Hoe doen we dat?

Stichting Surplus hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het schoolbestuur van Stichting Surplus 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. Stichting Surplus voldoet aan alle relevante wet- en regelgeving (zie paragraaf 5.1).

3. Bij Stichting Surplus is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één (of meerdere) wettelijke grondslagen. Een goede balans tussen het belang van Stichting Surplus 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 eerder gegeven toestemming intrekken of alsnog toestemming geven

4. Stichting Surplus 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. Stichting Surplus legt alle verwerkingen van persoonsgegevens vast in een verwerkingsregister en zal deze up-to-date houden.

6. Binnen Stichting Surplus 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. Leerlingen, ouders/verzorgers en medewerkers worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.

8. Stichting Surplus classificeert informatie en informatiesystemen. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen beveiligingsmaatregelen. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen en de te nemen maatregelen.

9. Stichting Surplus sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de stichting, persoonsgegevens verwerken. Dit geldt ook voor andere organisaties indien er gegevens van leerlingen of medewerkers worden verstrekt.

10. Stichting Surplus verwacht van alle leerlingen, ouders/verzorgers, medewerkers, (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 imagoverlies. Stichting Surplus heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.

11. Informatiebeveiliging en privacy is bij Stichting Surplus een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

12. Stichting Surplus 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. Stichting Surplus 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.
    Als de infrastructuur elders wordt beheerd en/of gegevens elders worden verwerkt legt Stichting Surplus aanvullende afspraken vast over de technische maatregelen.

14. Stichting Surplus zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

5 Uitwerking van het beleid – Wat doen we?

Dit hoofdstuk geeft een praktische invulling van bovenstaande beleidspunten.

5.1 Relevante wet- en regelgeving

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

- Wet op het primair onderwijs
- Wet goed onderwijs en goed bestuur PO
- Wet onderwijstoezicht
- (Uitvoeringswet) Algemene Verordening Gegevensbescherming
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

De norm voor informatiebeveiliging Baseline Informatiebeveiliging Overheid (BIO) (www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid) is leidend voor de te nemen beveiligingsmaatregelen.

De bepalingen van de meest recente versie van het privacy convenant onderwijs 'Digitale onderwijsmiddelen en privacy' (www.privacyconvenant.nl) zijn leidend bij het maken van afspraken met leveranciers, die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerken.

5.2 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.

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 (subsidiar). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.
4. **Transparantie**: Stichting Surplus legt aan betrokkenen 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.

5.3 Ondersteunende richtlijnen en procedures

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

5.4 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 leerlingen, ouders/verzorgers en medewerkers. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de verantwoordelijke IBP, de FG, en de privacy officer met het bestuur als eindverantwoordelijke.

5.5 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 het type gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de aspecten 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.

5.6 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 via het meldingsformulier.
Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden. Deze maakt onderdeel uit van de PDCA-cyclus.

5.7 Planning en control

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.

Daarnaast kent Stichting Surplus een jaarlijkse PDCA-cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst en eventueel aangepast of verbeterd. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving et cetera meegenomen.

5.8 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 en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode, 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 aangesteld door het bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het bestuur vast te stellen reglement.

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

5.9 Logging en monitoring

Logging en monitoring door de IT-afdeling zorgt ervoor 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.

6 Organisatie - Wie doet wat?

6.1 Rollen en verantwoordelijkheden

Het IBP-beleid gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol. Onderstaand overzicht geeft aan welke verantwoordelijkheden en taken bij welke rollen horen bij Stichting Surplus.

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 vaststellen • Privacyreglement vaststellen • Privacyverklaring vaststellen • Reglement FG vaststellen
Sturend (tactisch)	Privacy officer	• Inhoudelijk verantwoordelijk voor IBP • IBP-planning en controle • Adviseert 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 • Incidentafhandeling (registreren en evalueren). • Voorlichting privacy en stimuleren bewustwording	Processen, richtlijnen en procedures IBP, waaronder: • Activiteitenkalender • Protocol datalekken en datalekregister • Verwerkersovereenkomsten regelen • Brief toestemming gebruik beeldmateriaal • Opstellen informatie documentatie richting leerlingen, ouders/verzorgers • Security awareness activiteiten • Gedragscode medewerkers en leerlingen • Bijhouden verwerkingsregister • risicoanalyse uitvoeren • PDCA-cyclus (organisatie verbetercirkel) • Bijhouden en opstellen beveiligingsincident beheer

Sturend (tactisch)	Functionaris voor Gegevens-bescherming	• Toezicht op naleving privacy wetgeving • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Afwikkeling klachten en vragen van betrokkenen • Draagt zorg voor het verbeteren en stimuleren van bewustwording rondom IBP • Gevraagd en ongevraagd advies • Ambassadeur voor juiste toepassing privacywetgeving in de organisatie	• Rapportage CvB
	Afdelingen: • ICT • HRM / P&O • Facilitair • Onderwijs • Financiën • Administratie	• Classificatie/risicoanalyse in samenwerking privacy officer • 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); input dataregister • Classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk
Uitvoerend (operationeel)	Functioneel en/of applicatie beheerder Medewerker Leidinggevende	• Uitvoeren taken conform gegeven richtlijnen en procedures. • Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden. • Communicatie naar alle betrokkenen; ervoor 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.: • IBP in het algemeen • Regels passend onderwijs • Hoe omgaan met leerling dossiers • Wie mogen wat zien • Gedragscode • Omgaan met sociale media • Mediawijs maken

De verdere uitwerking van de rollen en taken staan beschreven in bijlage 2.

Bijlage 1: Ondersteunende richtlijnen en procedures

Een aantal aanvullende beleidsstukken, richtlijnen, procedures en protocollen, zijn:

- Privacyreglement
- Privacyverklaring (communicatie richting betrokkenen)
- Gedragscode voor de medewerkers
- Diverse schoolspecifieke stukken (o.a. gedragscode leerlingen, gedragscode ouders/verzo gers, toestemmingsformulier gebruik beeldmateriaal en procedure rondom uitwisselen gegevens)
- Protocol datalekken
- Registratie beveiligingsincidenten
- Verwerkingsregister
- Verwerkersovereenkomsten (privacy bijlage beschikbaar stellen)
- Procedure rondom training medewerkers (bewustzijn creëren)
- Functionaris voor Gegevensbescherming (communicatie hierover richting medewerkers)
- Risicoanalyse
- Procedure voor verwijderen van gegevens (bewaartermijnen)
- Procesbeschrijving rechten betrokkenen (proces rondom aanvragen van betrokkenen)
- Autorisatiematrix (wie mogen gegevens inzien, bewerken enz.)
- PDCA-cyclus (organisatie verbetercirkel)
- Procedure gegevensbeschermingseffectbeoordeling (DPIA)

Bijlage 2: Organisatie; wie doet wat

Deze bijlage beschrijft hoe IBP op drie niveaus wordt georganiseerd.

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

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij stichting Surplus voor elk niveau een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen.
Beschreven wordt wie welke rollen, welke verantwoordelijkheden en welke taken hebben en wat de documenten zijn die daarbij passen.

Richtinggevend

Eindverantwoordelijke
Het College van Bestuur is eindverantwoordelijk voor IBP en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast.
De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages geëvalueerd.
De inhoudelijke verantwoordelijkheid voor IBP is gemandateerd aan de privacy officer.

Sturend

Privacy officer
Privacy officer is een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke (het CvB) en stuurt de mensen aan op uitvoerend niveau. De privacy officer moet:

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

Functionaris voor Gegevensbescherming
De functionaris voor gegevensbescherming (FG) houdt binnen stichting Surplus toezicht op de toepassing en naleving van de AVG. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. De FG zorgt voor het verbeteren en stimuleren van bewustwording rondom IBP, adviseert over het regelen van privacy, onderhoudt zo nodig de contacten met de Autoriteit Persoonsgegevens (AP) en rapporteert aan de eindverantwoordelijke (het CvB). De FG heeft regelmatig overleg met de privacy officer. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen.

ICT beheer
Adviseert samen met de privacy officer de eindverantwoordelijke (het CvB) en is verantwoordelijk voor het organiseren van ICT en informatiebeveiliging binnen stichting Surplus.

Afdelingen
Binnen stichting Surplus zijn er verschillende afdelingen (ict, personeel (HRM, P&O), administratie, facilitaire- en financiële zaken, onderwijs en de scholen). Op elk van deze afdelingen is iemand verantwoordelijk (afdelingshoofd/directeur) om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.

Het afdelingshoofd/directeur is tevens verantwoordelijk voor de risico's die veroorzaakt worden doordat personen of applicaties ten onrechte toegang krijgen tot applicaties. Om deze risico's te verkleinen hebben afdelingshoofden/directeuren de volgende specifieke taken:

- Samen met de eindverantwoordelijke (het CvB) stellen zij het beleid voor toegang (autorisaties) vast.
- Samen met functioneel beheer en ICT-beheer zien zij er op toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn en voor hun werkzaamheden toegang toe moeten hebben.
- Samen met functioneel beheer en ICT-beheer beoordelen zij periodiek de toegangsrechten van de gebruikers.

Uitvoerend

Functioneel beheerder of Applicatiebeheerder
Ieder softwarepakket of (web-)applicatie heeft een beheerder. Bij vragen over de software of applicatie is bekend wie daarvoor aangesproken kan worden. De functioneel beheerder wordt vanuit het afdelingshoofd of directeur voorzien van een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert hij zijn of haar taken uit.
.
Medewerker
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. het personeelshandboek en de gedragscode. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.
Medewerkers worden 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 MR).

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 IBP-beleid;
- 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 privacy officer. Leidinggevenden hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.