AVG 2018-2022

Stichting ISA
Islamitische basisscholen al Jawhara - al Yaqoet - al Maes

Inhoud

Inleiding

Het onderwijsveld is in toenemende mate afhankelijk van informatie en (meestal geautomatiseerde) informatievoorzieningen. Ook neemt de hoeveelheid informatie toe door ontwikkelingen als gepersonaliseerd leren met ict. Deze afhankelijkheid van ict en gegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het is van belang om adequate maatregelen te nemen op het gebied van **i**nformatie**b**eveiliging en **p**rivacy (**IBP**) 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.

Onder **informatiebeveiliging** wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten van de informatievoorziening te garanderen.
Deze aspecten zijn:

1. **Beschikbaarheid**: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
2. **Integriteit**: de mate waarin gegevens en/of functionaliteiten juist en volledig zijn.
3. **Vertrouwelijkheid**: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

Onvoldoende informatiebeveiliging kan leiden tot onacceptabele risico's bij de uitvoering van onderwijs en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

Privacy gaat over persoonsgegevens. Persoonsgegevens dienen beschermd te worden conform huidige wet – en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens gebruikt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die herleidbaar zijn tot een bepaald individu. Onder verwerking wordt verstaan elke handeling met betrekking tot persoonsgegevens. 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.*

Uit voorgaande blijkt dat informatiebeveiliging een belangrijk onderdeel is van privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Beide begrippen staan naast elkaar, en zijn van elkaar afhankelijk. Dit beleid ligt ten grondslag aan de aanpak van IBP binnen de scholen die ressorteren onder ***Stichting Islamitische School Amsterdam***: **IBS Al Maes, IBS Al Jawhara en IBS Al Yaqoet**.

1. Doel

Dit beleid heeft als doelen:

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

Dit beleid is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij een goede balans moet zijn tussen privacy, functionaliteit en veiligheid. Uitgangspunt is dat de persoonlijke levenssfeer van de betrokkenen, medewerkers, leerlingen en ouders, wordt gerespecteerd en de school (IBS Al Maes/ IBS Al Jawhara /IBS Al Yaqoet) voldoet aan relevante wet- en regelgeving.

2. Reikwijdte

- Het informatiebeveiligings- en het privacy (IPB) beleid binnen de school geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), alsmede voor alle organisatieonderdelen. Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.
- De nadruk van het beleid ligt op die toepassingen, die vallen onder de verantwoordelijkheid van de school. Het beleid heeft zowel betrekking op gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd. Daarnaast is het ook van toepassing op niet-gecontroleerde informatie waarop de school kan worden aangesproken, zoals uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites.
- Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen de school waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op andere betrokkenen waarvan de school persoonsgegevens verwerkt.
- In het IBP-beleid ligt de nadruk op de, geheel of gedeeltelijk, geautomatiseerde /systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van de school evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het 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 binnen de school heeft 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.
- **IT-beleid**; met als aandachtspunten aanschaf, beheer en gebruik van ICT en (digitale) leermiddelen.
- **Medezeggenschap** van ouders/verzorgers en medewerkers.
- Beleid inzake aanschaf en gebruik van digitale leermiddelen.

3. Algemene beleidsuitgangspunten van AVG

De belangrijkste **beleidsuitgangspunten van AVG** bij de school (IBS al Maes/ IBS al Jawhara / IBS al Yaqoet) zijn:

1. Informatiebeveiliging en het privacy dient te voldoen aan alle relevante wet- en regelgeving, in het bijzonder aan de Wet Bescherming Persoonsgegevens (WBP) en de **A**lgemene **V**erordening **G**egevensbescherming (AVG), die 25 mei 2018 in werking is getreden. De verwerking van persoonsgegevens is gebaseerd op één van de wettelijke grondslagen. Waarbij een goede balans tussen het belang van de school om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn persoonsgegevens van belang is (zie bijlage 9: *Privacyreglement voor scholen van Stichting ISA* en bijlage 19*: Protocol social media*).

2. Binnen de school 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 fysieke documenten (zie bijlage 10: *Geheimhoudingsovereenkomst voor de scholen van Stichting ISA* en bijlage 15: *Gebruik beeldmateriaal leerlingen*).

3. De school is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers, leerlingen en ouders worden goed geïnformeerd over de regelgeving rond het gebruik van informatie (zie bijlage 8: *Procesbeschrijving rechten betrokkenen* en bijlage 19*: Protocol social media* en bijlage 16: *Informatieplicht*).

4. Informatie heeft een waarde: financieel, economisch maar zeker ook emotioneel. Op school wordt de waarde van informatie geclassificeerd. De classificatie is het uitgangspunt voor de te nemen maatregelen. Vervolgens worden mogelijke risico's geïdentificeerd middels een risicoanalyse, waarbij gebruik wordt gemaakt van de classificatie. Er is een balans tussen de risico's van hetgeen we willen beschermen en de benodigde investeringen en maatregelen (zie bijlage 2: *BIV-classificatie, bijlage 3: Risicoanalyse* en bijlage 17: *Risicoanalyse waarom?*).

5. De school sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) bewerkersovereenkomsten af als zij persoonsgegevens ontvangen van de school. Hierbij wordt gebruik gemaakt van de meest recente versie van het convenant '*Digitale leermiddelen privacy*' (www.privacyconvenant.nl) en de bijbehorende model bewerkersovereenkomst. Dit geldt ook voor overheids- en andere instellingen indien er gegevens van leerlingen of medewerkers worden verstrekt, al dan niet op wettelijke basis (zie bijlage 14: *Bewerkersovereenkomst*).

6. Er wordt van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties verwacht 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. De school heeft hiervoor een gedragscode geformuleerd (zie bijlage 18*: Gedragscode gebruik informatievoorziening*), vastgesteld en geïmplementeerd (zie bijlage 5: *Protocol informatiebeveiligingsincidenten en datalekken van Stichting ISA,* bijlage 13: *Responsible disclosure* en bijlage 19*: Protocol social media*.

7. IPB is op school een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is (zie bijlage 4: *Jaarkalender*).

8. Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt op school vanaf de start rekening gehouden met IBP (zie bijlage 11: *Transparantie over privacy Stichting ISA*).

Het pdfbestand bijlage ***'aandachtspunten AVG'*** gaat in op de gevolgen die de uitgebreide (U) en nieuwe (N) regels van de AVG hebben voor de school, wat je moet regelen en hoe de aanpak IBP je hierbij kan helpen. Een aantal (complexe) handreikingen om te voldoen aan de AVG zijn in de laatste kolom in lichtgrijze tekst opgenomen.

4. Uitgangspunten privacy

De vijf vuistregels met betrekking tot de omgang van persoonsgegevens op school zijn:

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. Doel en doelbinding is vastgesteld in het beleid en in privacyreglement. Art. 19 Vrijstellingsbesluit Wbp geeft toegestane doeleinden van verwerking voor scholen. AVG vereist welke persoonsgegevens dienen te worden vastleggen voor welke doelen gebruikt worden, hoe lang deze bewaard worden enz.
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. Verwerking vindt doorgaans plaats op basis van wet, wettelijke taak of gerechtvaardigd belang. AVG vereist dat er toestemming dient te worden gevraagd voor het gebruik van beeldmateriaal van leerlingen.
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 (= subsidiair). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk, niet meer gegevens vragen dan strikt noodzakelijk is en niet langer verwerken mag worden dan nodig om het doel te behalen.
4. **Transparantie**: de school legt aan betrokkenen (leerlingen en hun ouders, medewerkers en (geregistreerde) bezoekers) 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. Alle betrokkenen moeten vooraf in begrijpelijke taal geïnformeerd worden over welke informatie voor welk doel verwerkt wordt en wat hun rechten en plichten zijn. Procedures zijn geregeld in het privacyreglement. (Zie bijlage 11: *Transparantie over Privacy Stichting ISA,* bijlage 9: *Privacyreglement voor scholen van Stichting ISA* en bijlage 8: *Procesbeschrijving rechten betrokkenen,*
5. **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn. (Zie bijlage 12: *Wachtwoord beleid* en bijlage 16: *Informatieplicht*). Persoonsgegevens worden adequaat beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen. Bij alle registraties op basis van toestemming, zal de school aan de betrokkene een eenduidige zogenaamde Opt-out procedure worden aangeboden (zie bijlage 6: *Incidenten registratie Stichting ISA*).

5. Wet en regelgeving

De school 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.

6. Organisatie

De organisatie van IBP 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.
In bijlage 1 (*Tabel IBP rollen en taken*) wordt beschreven hoe IBP op school is georganiseerd. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

1. **Richtinggevend** (strategisch)
2. **Sturend** (tactisch)
3. **Uitvoerend** (operationeel)

Voor elk niveau wordt hieronder en bijlage 1 beschreven welke rollen welke verantwoordelijkheden en taken hebben en wat de documenten zijn die daarbij passen:

7. Rollen (functies) rondom IBP

Om IBP gestructureerd en gecoördineerd op te pakken worden op school een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen (zie bijlage 1: *Tabel IPB rollen en taken*).

8. Richtinggevend

De **directeur-bestuurder** is eindverantwoordelijk voor IBP en stelt het beleid en de basismaatregelen op het gebied van IBP 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 manager IBP.

9. Sturend

De volgende functionarissen hebben sturende functie:

Manager IBP

Manager IBP is een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke en stuurt de mensen aan op uitvoerend niveau. De manager IBP moet:

- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling;
- De uniformiteit bewaken binnen de school;
- Is het aanspreekpunt voor incidenten op het gebied van informatiebeveiliging en privacy;
- Coördineert de verdere afhandeling van incidenten binnen de school.

Functionaris voor Gegevensbescherming (FG)

De functionaris voor gegevensbescherming (FG) houdt binnen het schooltoezicht 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 afhandelen van vertrouwelijke informatiebeveiligingsincidenten.
De FG heeft regelmatig overleg met manager IBP.
De FG is meestal ook de contactpersoon voor klachten en vragen van betrokkenen.

Portefeuillehouder ICT/ICT beheer
ICT-beheerder adviseert samen met manager IBP/informatiemanager de directeur-bestuurder en is verantwoordelijk voor het organiseren van ICT en informatiebeveiliging binnen de school.

Domeinverantwoordelijke/proceseigenaar
Binnen de school zijn er verschillende domeinen/processen, zoals ict, personeel (HRM, P&O), administratie, facilitaire- en financiële zaken, onderwijs 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.
Deze proceseigenaar 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 proceseigenaren de volgende specifieke taken:

- Samen met de directeur-bestuurder stellen zij het beleid voor toegang vast.
- Samen met functioneel beheer en ICT-beheer zien zij erop toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.
- Samen met functioneel beheer en ICT-beheer beoordelen zij regelmatig de toegangsrechten van gebruikers.

Leidinggevenden hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.

10. Uitvoerend

De volgende functionarissen hebben uitvoerende functie:

Functioneel beheerder (FB)
De functioneel beheerder wordt vanuit de domeinverantwoordelijke/proceseigenaar voorzien van een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert hij/zij zijn/haar taken uit.

Medewerker
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. het personeelsboek en de handleiding acceptabel gebruikmaken van bedrijfsmiddelen. 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 (G)MR)

Leidinggevende
Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft op uitvoerend niveau de taak om:

- Ervoor 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.

11. Controle en rapportage

Dit IPB-beleid 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 de school een jaarlijkse planning en control cyclus voor IPB. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het IPB-beleid wordt getoetst.

Voor alle overlegmomenten geldt dat deze zoveel mogelijk ingepast worden in bestaande overlegvormen met hetzelfde karakter waarbij op:

- **Strategisch** niveau richtinggevend wordt gesproken over organisatie en compliance, alsmede over doelen, scope en ambitie op het gebied van IBP.
- **Tactisch** niveau wordt de strategie vertaald naar plannen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering.
- **Operationeel** niveau worden de onderwerpen besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan. Deze overlegvorm wordt decentraal georganiseerd, en indien nodig in elk organisatieonderdeel van de school.

12. Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van IBP uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt op school 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 FB met directeur-bestuurder als eindverantwoordelijke. De powerpoint presentaties '*AVG presentatie'* en *'Presentatie – IPB voor medewerkers'* worden hierbij gebruikt.

13. Classificatie en risicoanalyse

De school heeft alle informatiewaarde, 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 (zie bijlage 2: *BIV - Classificatie* en bijlage 3: *Risicoanalyse*).

14. Incidenten en datalekken

Alle incidenten kunnen worden gemeld bij **helpdesk@as-siddieq.nl**. De afhandeling van deze incidenten volgt een gestructureerd proces, die ook voorziet in de juiste stappen rondom de meldplicht datalekken (zie bijlage 5: *Protocol informatiebeveiliging en datalekken van Stichting ISA*).

15. 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. Op school 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 voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door de directeur-bestuurder, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door de directeur-bestuurder vast te stellen reglement.

Mocht de naleving ernstig tekortschieten, dan wordt de betrokken verantwoordelijke medewerkers een sanctie opgelegd, binnen de kaders van de CAO en de wettelijke mogelijkheden. Op school is het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol.

Bijlagen

Bijlage 1: Tabel IBP rollen en taken

Niveau	Wie Rollen	Hoe Verantwoordelijkheid/taken	Wat Realiseren/vastleggen
Richtinggevend (strategisch)	Directeur-bestuurder	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 (IPB) beleid Baseline/basismaatregelen Reglement FG vaststellen Privacyreglement vaststellen
Sturend (tactisch)	Manager IBP	Inhoudelijk verantwoordelijk voor IBP IBP-planning en controle Adviseert algemeen bestuur/directeur-bestuurder/directie van de scholen 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: 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 (FG) / Privacy officer	Toezicht op naleving privacywetgeving 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
	Domeinverantwoordelijke/ Proceseigenaren waaronder: ict, personeel (HRM/P&O), Facilitair, onderwijs , financiën, inkoop en administratie	**Classificatie/risicoanalyse** *in samenwerking met Manager IBP (Informatiemanager/verantwoordelijke IBP)* Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door directeur-bestuurder *Samen met functioneel beheer en ICT-beheer* erop 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
Niveau	**Wie Rollen**	**Hoe Verantwoordelijkheid/taken**	**Wat Realiseren/vastleggen**

			Vanuit de Wiki
Uitvoerend (operationeel)	Functioneel beheerder Medewerker	Incidentafhandeling (registreren en evalueren). Technisch aanspreekpunt voor IBP-incidenten. Uitvoeren taken conform gegeven richtlijnen en procedures. Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden.	Communiceren, informeren en toezien op naleving van o.a.:
	Dagelijkse leiding/leidinggevende /directie	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.	IBP in het algemeen Regels passend onderwijs Hoe omgaan met leerling dossiers Wie mogen wat zien Gedragscode Omgaan met sociale media Mediawijs maken

In de IBP kom je de volgende functies, rollen en taken tegen. In de tabel hierboven zijn wie/hoe/wat beschreven. De kolom **'wie'** geeft aan welke rol de genoemde verantwoordelijkheden/ taken op zich kan nemen.
- Op **strategisch niveau** is de directeur-bestuurder verantwoordelijk om IBP goed te regelen en daarmee ook om de IBP organisatie goed in te richten.
- Een **manager informatiebeveiliging en privacy** (afgekort als manager IBP) is een rol op strategisch, tactisch en operationeel niveau. Hij/zij adviseert o.a. de directeur- bestuurder. De manager IBP bewaakt de uniformiteit op het gebied van IBP binnen de instelling.
- Een **proces eigenaar** is iemand die verantwoordelijk is voor één van de primaire of ondersteunende processen, zoals HRM/P&O, administratie, financiën of onderwijs.
In de kolom **'hoe'** staat aangegeven welke verantwoordelijkheden en taken er minimaal belegd moeten worden
De kolom **'wat'** geeft de praktische uitwerking van het beleid op elk niveau weer. Welke processen worden erdoor wie beschreven, wie legt welke afspraken vast, wie keurt deze goed en hoe wordt er gecommuniceerd.

Extra aandacht vragen de volgende punten:

Toegang en toegangsbeleid

Het is voor IBP héél belangrijk om te weten wie waarbij mag en wie daarover uiteindelijk de beslissingen neemt. Daarom is het goed om iemand specifiek hiervoor verantwoordelijk te maken.

Individuele medewerkers

Degene die het meest in aanraking komen met persoonsgegeven, zijn de medewerkers. Zij leggen veel gegevens van leerlingen vast om ze op de juiste manier te kunnen begeleiden en ook administraties verwerken veel persoonsgegevens. Het is daarom belangrijk dat alle medewerkers het belang van IBP inzien en erkennen. Zij worden dan ook zoveel mogelijk bij het hele proces betrokken.

Bijlage 2: BIV- Classificatie

De kwaliteitsaspecten die worden toegepast op informatiebeveiliging zijn:
1. Beschikbaarheid,
2. Integriteit, en
3. Vertrouwelijkheid.

Deze termen worden hier, inclusief de deelaspecten, beschreven. Alle aspecten kunnen worden geclassificeerd in laag, midden en hoog.

Ad1. Beschikbaarheid: de mate waarin beheersmaatregelen de beschikbaarheid en ongestoorde voortgang van de ict-dienstverlening waarborgen.
Deelaspecten hiervan zijn:
• **Continuïteit**: de mate waarin de beschikbaarheid van de ict-dienstverlening gewaarborgd is;
• **Portabiliteit**: de mate waarin de overdraagbaarheid van het informatiesysteem naar andere gelijksoortige technische infrastructuren gewaarborgd is;
• **Herstelbaarheid**: de mate waarin de informatievoorziening tijdig en volledig hersteld kan worden.
Voor de beschikbaarheid komt de classificatie *laag, midden en hoog* respectievelijk overeen met *niet vitaal, vitaal en zeer vitaal.*

Ad2. Integriteit: de mate waarin de beheersmaatregelen (organisatie, processen en technologie) de juistheid, volledigheid en tijdigheid van de IT-dienstverlening waarborgen.
Deelaspecten hiervan zijn:
• **Juistheid**: de mate waarin overeenstemming van de presentatie van gegevens/informatie in IT-systemen ten opzichte van de werkelijkheid is gewaarborgd;
• **Volledigheid**: de mate van zekerheid dat de volledigheid van gegevens/informatie in het object gewaarborgd is;
• **Waarborging**: de mate waarin de correcte werking van de IT-processen is gewaarborgd.
Voor de integriteit komt de classificatie *laag, midden en hoog* respectievelijk overeen met *openbaar, intern en vertrouwelijk.*

Ad3. Vertrouwelijkheid: de mate waarin uitsluitend geautoriseerde personen, programmatuur of apparatuur gebruik kunnen maken van de gegevens of programmatuur, al dan niet gereguleerd door (geautomatiseerde) procedures en/of technische maatregelen.
Deelaspecten hiervan zijn:
• **Autorisatie**: de mate waarin de adequate inrichting van bevoegdheden gewaarborgd is;
• **Authenticiteit**: de mate waarin de adequate verificatie van geïdentificeerde personen of apparatuur gewaarborgd is;
• **Identificatie**: de mate waarin de mechanismen ter herkenning van personen of apparatuur gewaarborgd zijn;
• **Periodieke controle op de bestaande bevoegdheden**. Het (geautomatiseerd) vaststellen of geïdentificeerde personen of apparatuur de gewenste handelingen mogen uitvoeren.
Voor de vertrouwelijkheid komt de classificatie *laag, midden en hoog* respectievelijk overeen met *openbaar, intern en vertrouwelijk.*

Hoe bepaal ik het classificatie niveau?
Hiervoor maken we gebruik van de vragen, zoals deze zijn opgesteld voor het certificeringsschema

Bijlage 3: Risicoanalyse

De AVG eist van de school dat zij bewust omgaat met privacy. Hierbij hoort het in kaart brengen van de huidige situatie rondom IBP. De school moet zich daarbij niet alleen aan de wet houden, maar ook kunnen aantonen dat zij dat doet. In het Excel bestand '*Risicoanalyse'* is een risicoanalyse voor de school uitgevoerd. En powerpoint presentatie '*korte uitleg risicoanalyse*' laat zien wat risicoanalyse inhoudt.

Huidige situatie

Waar liggen op dit moment de grootste risico's? Door het uitvoeren van een risicoanalyse hebben we dit in beeld gebracht. Hiermee bepalen we eerst wat de (grootste) risico's zijn. Daarna kijken we welke maatregelen nodig zijn om die risico's tot een minimum te beperken. Deze maatregelen kunnen we vervolgens samen met de wettelijke verplichtingen inplannen voor de komende tijd.
De risicoanalyse geeft antwoord geven op de vragen:
1. Wat zijn de grootste risico's bij gebruik van het leerling administratiesysteem? En welke maatregelen zijn nodig om deze risico's te beperken?
2. Wat zijn de risico's bij het inzetten van sociale media in de klas? Welke maatregelen moeten we nemen om dat goed te regelen?

Een risicoanalyse heeft niet alleen de grootste risico's aan het licht gebracht, maar het is ook een middel om te zorgen dat iedereen hetzelfde beeld krijgt over risico's en de nadelige gevolgen voor de school, zodat we als school weten waar we als eerste in moet investeren, nl:
1. **Reputatieschade**: door incidenten die gemeld worden in de media. Bijvoorbeeld examenfraude, wachtwoorden op straat, gestolen examens. Dit is slecht voor het imago van een school.
2. **Financiële schade**: als leerlinggegevens niet juist zijn kan de bekostiging van deze leerlingen in gevaar komen; je niet houden aan de privacywetgeving kan financiële consequenties hebben, zoals het niet melden van een datalek.
3. **Continuïteit** in het onderwijs: Cybercrime en DDos-aanvallen kunnen het onderwijs enorm verstoren.
4. **Wet en regelgeving**: er moet aantoonbaar voldaan worden aan de AVG.
5. Risico's in de **cloud**: toepassingen in de cloud leveren specifieke aandachtspunten op zoals eigenaarschap, toegang, privacy en continuïteit van de dienstverlening van externe partijen.
6. Te beperkt **kennisniveau**: ontwikkelingen gaan snel, de eisen om te voldoen aan wet- en regelgeving worden strenger en de risico's groter. Onvoldoende kennis kan tot gevolg hebben dat er onjuiste beslissingen worden genomen ten aanzien van IBP met alle gevolgen van dien.

Bijlage 4: Jaarkalender

(In het Excel bestand '*incidentenregistratie st.ISA*' is de jaarkalender te vinden)

Bijlage 5: Protocol informatiebeveiligingsincidenten en datalekken van Stichting ISA

Inleiding
Het Protocol informatiebeveiligingsincidenten en datalekken sluit aan bij de uitgangspunten in het IPB-beleid van Stichting Islamitische School Amsterdam (ISA). Dit protocol biedt een handleiding voor **de professionele melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken**. Het doel hiervan is het voorkomen van beveiligingsincidenten en datalekken. En dit protocol is van toepassing op de gehele organisatie van Stichting ISA zoals het vermeld is in het IBP-beleid en al haar medewerkers.

Gebruikte termen:

- **Beveiligingsincident**; een beveiligingsincident is een gebeurtenis die ervoor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast.
- **Informatievoorziening**; het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van de organisatie.
- **Datalek**; een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden, et cetera). Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.
- **Betrokkene**; de persoon van wie de persoonsgegevens zijn gelekt.

Wet- en regelgeving datalekken
Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht zijn ook scholen verplichting melding te maken van ernstige datalekken bij de Autoriteit Persoonsgegevens. Vanaf 25 mei 2018 (ingangsdatum Algemene Verordening Gegevensbescherming (AVG) kan het nalaten van deze melding leiden tot een fikse boete.

De meldplicht is alleen van toepassing wanneer persoonsgegevens worden verwerkt, bijvoorbeeld in leerling administratie of digitale leermiddelen. De school heeft aanvullende afspraken gemaakt over het melden van datalekken met bewerkers, leveranciers, zoals uitgevers of distributeurs, die persoonsgegevens ontvangen van de school.

Er is sprake van een datalek als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben. Een datalek is het gevolg van een beveiligingsprobleem, verkeerd gebruik of een verlies. Het kan gaan om gestolen computerbestanden (gehackt), al kan een gestolen geprinte klantenlijst evengoed een datalek vormen.
Voorbeelden in onze school zijn: het verlies/diefstal van een usb stick, het verlies/diefstal van een laptop of telefoon (ook privé), het verlies/slordig omgaan met vertrouwelijke prints. Maar het verliezen van een usb-stick met daarop de adresgegevens van klas 3b, is ook een datalek.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is de directeur-bestuurder. Een leverancier is een bewerker voor de school. De afspraak op school is dat een bewerker namens de verantwoordelijke de melding doet, maar dat gebeurt dan onder verantwoordelijkheid van de directeur-bestuurder.

Als er een datalek is, wordt daar binnen 72 uur na ontdekking van de lek melding van gedaan bij de Autoriteit Persoonsgegevens.

Hoe voorkom je datalekken?

- Gebruik op het werk andere wachtwoorden dan privé. Wijzig regelmatig je wachtwoorden.
- Kies nooit een eenvoudig wachtwoord en bewaar deze gegevens veilig.
- Geef aan niemand je logingegevens.
- Wanneer je een melding krijgt dat je laptop moet geüpdatet worden stel dat dan niet uit.
- Sluit af of vergrendel je laptop wanneer je je laptop even achterlaat.
- Gebruik niet meer gegevens dan nodig. Verzamel geen persoonsgegevens die geen waarde toevoegen.
- Wees extra zorgvuldig bij het printen en kopiëren. Laat geen kopieën van persoonsgegevens/ privacygevoelige documenten bij de printer liggen; een verloren kopie moet gemeld worden.

- Indien een print gestuurd en deze is niet bij de printer aangekomen, kijk printerinstellingen na of de juiste printer gekozen is. Spoor de fout geprinte documenten op!
- Vind je documenten van een collega, -die persoonsgegevens bevatten- bv bij een printer, breng ze bij de collega en wijs deze op het feit dat dit open ter inzage lag.
- Bij verlies/diefstal van de (privé) smartphone, USB-stick/externe schijf en of tablet waarop werkmail gesynchroniseerd wordt direct melding maken bij de FG.
- Leen je laptop/telefoon niet aan onbevoegden.
- Op USB/externe harde schijf geen data met persoonsgegevens plaatsen. Indien het nodig is/was omdat het netwerk (Office 365) niet beschikbaar was/is direct nadat het weer beschikbaar is op het netwerk plaatsen en verwijderen van de usb stick.
- Bij verlies/diefstal van een USB/externe harde schijf waarop privacy gevoelige documenten staan, direct melding maken de FG. Gebruik hiervoor het stappenplan datalekken.
- Geen persoonsgegevens van leerlingen laptops plaatsen altijd op Cloud (Office 365).
- Bewaar nooit gevoelige data in een public Cloud, bijvoorbeeld: Dropbox, je privé Google Drive. Met communicatiemiddelen zoals Dropbox, WhatsApp kan informatie sneller in handen komen van derden. Verspreid geen persoonsgegevens via de e-mail en/of Clouddiensten waar geen contract mee is afgesloten zoals Dropbox. Hiervoor mag alleen Office 365 @as-siddieq.nl account gebruikt worden. Weeg dus goed af met welk middel je gevoelige informatie communiceert.
- Alleen mails verzenden vanuit onze eigen mailadressen (@as-siddieq.nl).
- Wees erg kritisch met openen en lezen van e-mails, kijk altijd eerst naar de afzender en als je deze niet kent wees dan op je hoede.
- Indien er toch documenten gemaild moeten worden met daarin persoonsgegevens. Beveilig het document met een wachtwoord. Check eerst het mailadres, bv door de ontvanger een mail te sturen met het verzoek deze te beantwoorden. Vervolgens kun je op die mail het document mailen. Je weet dan zeker dat je het juiste email adres hebt. Vraag voor de zekerheid een ontvangstbevestiging.
- Stuur geen mail met meerdere namen (bijv. alle cursisten) in CC maar altijd in BCC
- Bij twijfel van een of ander mogelijk verlies van data neem altijd contact op met de leidinggevende.

Afspraken met leveranciers

De directeur-bestuurder heeft als verantwoordelijke voor de persoonsgegevens afspraken gemaakt met leveranciers, die persoonsgegevens ontvangen. Afspraken over datalekken vallen daar ook onder. De school spreekt het volgende af:

- Hoe informeer je elkaar over datalekken, en zorg ook voor bereikbaarheid tijdens bijvoorbeeld het weekend en vakanties.
- Wie doet de melding bij de Autoriteit Persoonsgegevens.
- Welke informatiegegevens de bewerker moet geven bij een datalek.
- Welke informatie nodig is voor het doen van een melding, en dat je elkaar informeert over de melding (er wordt afgesproken dat er een kopie van de melding wordt ontvangen).
- De tijd waarbinnen de bewerkers de gegevens moet aanleveren.
- Wie de communicatie met de gebruikers voor haar rekening neemt als dat nodig is.

De school maakt schriftelijke afspraken met bewerker(s) over datalekken. Hiervoor wordt gebruik gemaakt van de modelbewerkersovereenkomst die hoort bij het convenant *'Digitale onderwijsmiddelen en privacy 2.0'* (www.privacyconvenant.nl).

Werkwijze

Uitgangssituatie

- Er is een actueel informatiebeveiligings- en privacy beleid;
- Er is een actueel document betreffende het aanvaardbaar gebruik van bedrijfsmiddelen en/of gedragscode ict en internetgebruik.

De vier rollen

Er zijn tenminste vier rollen die onderscheiden worden om een beveiligingsincident en/of datalek succesvol af te handelen:

- **Ontdekker (medewerker)**; degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
- **Meldpunt (servicedesk)**; een centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt.
- **Melder (functionaris gegevensbescherming)**; degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
- **Technicus (security officer/ict coördinator)**; degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

De zeven stappen

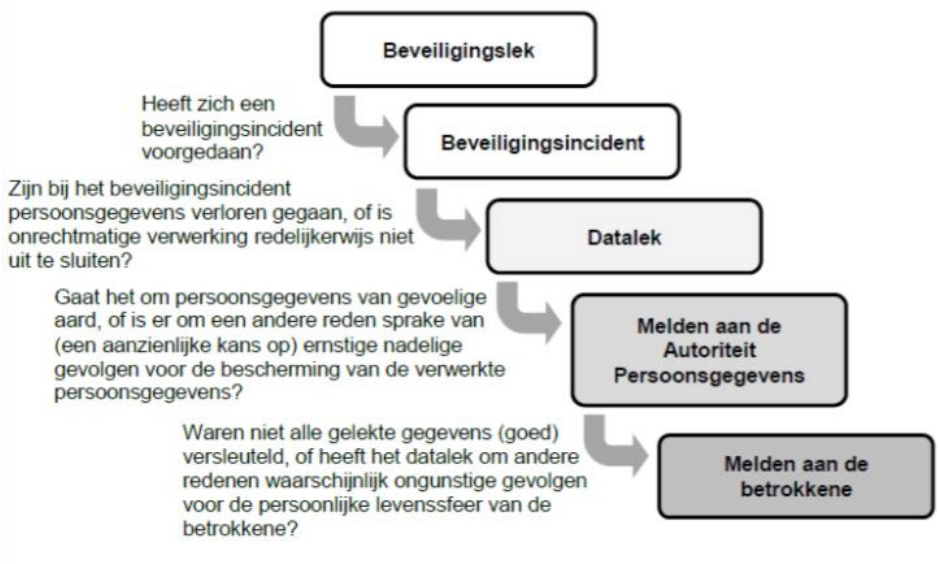
- **1. Ontdekken**
  De Ontdekker merkt een beveiligingsincident op. Via eigen waarneming of via waarneming van een derde. De Ontdekker verzamelt zoveel mogelijk informatie over het beveiligingsincident en meldt het bij het meldpunt via helpdesk@as-siddieq.nl

- **2. Inventariseren**
  Het Meldpunt bepaalt dan of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan zet hij aanvullende vragen uit bij de Ontdekker en/of de Technicus. De volgende informatie wordt daarna vastgelegd:
  - Samenvatting van het beveiligingsincident, wat is er met de gegevens gebeurd, wat voor gegevens zijn het (bijzondere gegevens of van gevoelige aard).
  - Datum/periode van het beveiligingsincident.
  - Aard van het beveiligingsincident.
  - Wanneer van toepassing (bij een datalek):
    - Omschrijving van de groep betrokkenen;
    - Aantal betrokkenen;
    - Type persoonsgegevens in kwestie;
  - Worden de gegevens binnen een keten gedeeld.

- **3. Beoordelen**
  Wanneer het Meldpunt voldoende informatie heeft verzameld, en een datalek vermoed, stuurt deze de Melder een verzoek om de verzamelde informatie te bekijken. De Melder beoordeelt de feiten om te bepalen of een melding aan de Autoriteit persoonsgegevens en/of betrokkenen vereist is.
  De volgende informatie wordt vastgelegd door de Melder:
  - Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen.
  - Wordt het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom niet?
  - Wordt het datalek aan betrokkenen gemeld? Waarom niet?
  - Hoe worden meldingen gedaan? Wat is de inhoud van de melding?

  Bij de beoordeling of er sprake is van een ‘meldingsplicht datalek’, houd je rekening met het type gegevens, en met de hoeveelheid gegevens. Indien het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens, dan moet er gemeld worden.

  Van die ernstige nadelige gevolgen of de kans op ernstige nadelige gevolgen is bijvoorbeeld sprake wanneer er heel veel gegevens van een betrokkene of gegevens van heel veel betrokkenen gelekt zijn maar ook wanneer de gelekte gegevens “gevoelig” zijn zoals bijvoorbeeld bijzondere persoonsgegevens over gezondheid, over de financiële of economische situatie van de betrokkene, of als de gegevens kunnen leiden tot stigmatisering van de betrokkene (denk aan het lekken van een leerling die vaak kinderen pest en daarmee gezien kan worden als notoire pester).



De bovenstaande beslisboom wordt gebruikt.

- **4. Repareren**
  De Technicus (intern of extern) wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De technicus van Stichting ISA legt onderstaande vast:
  - Technische en organisatorische maatregelen die genomen zijn om de inbreuk te verhelpen en verdere inbreuk te voorkomen. Voorgaande voor zover de oorzaak bekend is.
  - Zijn de gelekte gegevens onbegrijpelijk voor degenen die er kennis van heeft kunnen nemen? Hoe zijn de gegevens onbegrijpelijk gemaakt (versleuteld)?

- **5. Melden**
  Indien de conclusie bij stap 3 is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens (en eventueel betrokkenen), dan zal de Melder dit binnen twee werkdagen doen. De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen. Het lek wordt gemeld bij het **meldloket datalekken Autoriteit Persoonsgegevens**: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0.

- **6. Vastleggen**
  Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door het Meldpunt waarmee het incident is afgesloten. Het Meldpunt verstuurt een samenvatting van de genomen maatregelen aan de Ontdekker.

- **7. Informeren betrokkene: leerling en/of zijn ouders**
  Heeft het datalek waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene? Dan moet het datalek ook aan de betrokkenen zelf worden gemeld. Dat zijn medewerkers, leerlingen (of hun ouders als zij jonger zijn dan 16 jaar). In principe kan ervan worden uitgaan dat het lekken van gevoelige aard gelekt gemeld moet worden bij de betrokkenen. Als er persoonsgegevens zijn gelekt maar die zijn beveiligd of versleuteld, en de gelekte data zijn onbegrijpelijk of ontoegankelijk voor anderen, dan hoeft dat toch niet aan betrokkenen te worden gemeld. Bijvoorbeeld het lekken van een beveiligde én versleutelde database met gebruikersnamen en wachtwoorden.

Monitoring beveiligingsincidenten en datalekken
Het Meldpunt van Stichting ISA maakt twee keer per jaar een analyse van de meldingen van beveiligingsincidenten en datalekken in samenwerking met de functionaris gegevensbescherming. In de analyse wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen. De directeur-bestuurder wordt geïnformeerd over de uitkomsten van de analyse.

Communicatie
De school spreekt het volgende af:
- De manier van communiceren met betrokkenen en de pers.
- Hoe kan worden omgegaan met signalen van buitenaf over een mogelijk datalek.
- Is het inschakelen van externe deskundigen gewenst?

Formulier: melding datalekken aan betrokkenen

[Volledige naam betrokkene]
[Contactadres]
[Postcode plaats]

Plaatsnaam vestiging, datum

Betreft: Inlichtingen datalekken persoonsgegevens

Geachte [naam betrokkene],

Door middel van dit bericht wil ik je op de hoogte stellen van een inbreuk op de beveiliging van de data en persoonsgegevens bij organisatie. De inbreuk heeft invloed gehad op jouw persoonlijke persoonsgegevens. Aangezien wij waarschijnlijk ongunstige gevolgen voor je persoonlijke levenssfeer verwachten, lichten wij je in en willen wij je informatie verstrekken om de gevolgen te beperken.

Toelichting op aard van de inbreuk.
Als je meer informatie over de inbreuk wilt opvragen, kun je terecht bij naam instantie.

De inbreuk op de beveiliging en het datalekken kan ongunstige gevolgen hebben voor je persoonlijke levenssfeer. Om dit zo veel mogelijk te beperken bevelen wij je aan een aantal maatregelen te nemen. Aanbevolen maatregelen zijn: ……..

Wij hopen je met deze brief voldoende op de hoogte te hebben gebracht over de inbreuk en de gevolgen. Wij werken continue aan het verbeteren van de beveiliging en tegengaan van gevolgen van deze inbreuk. Onze excuses voor het ongemak dat je tot dusver hiervan hebt ondervonden.

Met vriendelijke groet,

Handtekening

Naam ondertekenaar,

Functie ondertekenaar

Bijlage 6: Incidenten registratie

(zie Excelbestand '*incidentenregistratie st.ISA*')

Bijlage 7: Rechten van betrokkenen

Door de Algemene Verordening Gegevensbescherming (AVG) krijgen betrokkenen (degenen van wie persoonsgegevens worden verwerkt) meer mogelijkheden om voor zichzelf op te komen als het gaat om de verwerking van hun gegevens. Onder de AVG zijn de rechten van betrokkenen verder uitgebreid.
Als het gaat om de rechten van betrokkenen is **transparantie** een belangrijke voorwaarde. Medewerkers, leerlingen en ouders (betrokkenen) worden actief betrokken en worden verteld wat hun rechten zijn. De school geeft betrokkenen de gelegenheid om hun rechten eenvoudig en met redelijke tussenpozen uit te oefenen. De school zorgt ervoor dat betrokkenen goed geïnformeerd zijn over hun rechten en de procedure om van hun rechten gebruik te kunnen maken.
Maar welke rechten hebben leerlingen en/of hun ouders (als de leerlingen jonger zijn dan 16 jaar) en medewerkers eigenlijk? In het document hieronder wordt dit verder uitgewerkt.

Transparantie en rechten betrokkenen

Transparantie is een belangrijke privacy-waarde. Daarom betrekt de school **leerlingen en/of zijn ouders en medewerkers (de betrokkene)** actief. De school legt uit, vertelt welke gegevens zij wil vastleggen of verstrekken aan externen en zegt ook waarom. Dit geldt ook voor de informatieoverdracht tussen scholen bij een overstap.
De school stelt de betrokkene in staat om bezwaren te uiten en zijn rechten uit te oefenen. Deze rechten zijn vastgelegd in de wet. De betrokkenen hebben de volgende rechten:

1. **Recht op informatie over gegevensverwerking**

Dit houdt in dat de betrokkene vooraf in begrijpelijke taal actief en laagdrempelig worden geïnformeerd over welke gegevens met welk doel worden verwerkt en wat de rechten van de leerling zijn.

2. **Recht op inzage, correctie, verwijdering/afscherming en bezwaar (verzet) van de persoonsgegevens**

De betrokkene heeft het recht op inzage van hun gegevens en het verbeteren of aanvullen van ontbrekende of verkeerd vastgelegde persoonsgegevens.

3. **Recht op verwijdering van de persoonsgegevens die niet (langer) nodig zijn om de vastgestelde doelen te behalen**

Het gaat alleen om gegevens die niet noodzakelijk zijn, of als het opslaan van die gegevens in strijd is met de wet.

4. **Recht van verzet tegen verwerking van persoonsgegevens bij de grondslag gerechtvaardigd belang, of verzet tegen direct marketing en profilering**

De betrokkene kan verzet instellen tegen een verwerking van zijn persoonsgegevens die plaats vond op grond van een gerechtvaardigd belang. De school maakt een afweging van het privacybelang van de betrokkene, tegenover het belang van de school om gegevens wél te gebruiken.
De betrokkene heeft het recht om bij toestemming, ook een beperkte toestemming te geven of toestemming te onthouden voor een onderdeel van de verwerking (**granulaire toestemming**).
De betrokkene heeft het recht dat verbeteringen, aanvullingen of verwijderingen aan alle andere partijen worden doorgegeven aan wie een organisatie de persoonsgegevens van betrokkene heeft verstrekt.

5. **Het recht op 'bevriezing van de verwerking' van zijn gegevens**

De betrokkene heeft het '**recht om te worden vergeten'** door het volledig wissen van de persoonsgegevens, tenzij er een wettelijke bewaarplicht geldt of het verwijderen in strijd is met de vrijheid van meningsuiting. Voor het onderwijs is dit recht minder relevant omdat we veel wettelijke bewaartermijnen gelden.
In geval van toestemming of een overeenkomst met de betrokkene, heeft de betrokkene het **recht op dataportabiliteit** als de verwerking van persoonsgegevens plaatsvindt op de grondslag toestemming. De school werkt niet veel met toestemming, daarom is dit recht minder relevant.

6. **Recht op melding datalek**

Bij een datalek heeft de betrokkene recht om daarover geïnformeerd te worden indien hij daar een zwaarwegend belang bij heeft.

7. **Recht van informatie over en verzet tegen geautomatiseerde besluitvorming**

De betrokkene heeft recht op 'profilering'.
(Zie powerpoint presentatie: *'AVG rechten van de betrokkenen'*)

Bijlage 8: Procesbeschrijving rechten betrokkenen

Leerlingen en/of ouders en medewerkers (de betrokkene) worden op het moment dat zij – voor het eerst – persoonsgegevens actief en bewust gaan delen met de school over hun rechten geïnformeerd. Er wordt verteld en uitgelegd welke gegevens er worden vastgelegd of doorgegeven aan een andere instantie en waarom. Alle betrokkenen weten dan hoe zij van hun rechten gebruik kunnen maken. In een procedure wordt vastgelegd hoe betrokkenen hun rechten kunnen uitoefenen. Rechten worden opgenomen in het leerlingenstatuut en/of in het privacyreglement. En het wordt ook op de website opgenomen met meer achtergrondinformatie over privacy en de rechten van betrokkenen.
In onderstaand document zijn de afspraken en procedures rondom de rechten van betrokkene op een rij gezet.

Privacyafspraken en -procedures

Een belangrijk onderdeel van privacy gaat over de rechten die betrokkene, leerlingen en/of ouders en medewerkers, heeft. Die rechten moet de betrokkene zelf kunnen uitoefenen binnen bepaalde termijnen. De school heeft een klachtenregeling waarin staat hoe betrokkene zijn rechten kan uitoefenen.
Belangrijkste zaken over de rechten van de betrokkene zijn:

1. Functionaris voor Gegevensbescherming (FG) is degene die de klachten van de betrokkenen in behandeling neemt.
2. Het verzoek van de betrokkene hoeft niet schriftelijk te zijn, dat mag ook digitaal of zelfs mondeling. De school legt wel altijd schriftelijk vast wat het verzoek is, en wanneer dat is ingediend.
3. De identiteit van de verzoeker moet duidelijk zijn, in geval ouders om inzage vragen moet vastgesteld kunnen worden dat het gaat om de wettelijk vertegenwoordigers (ouders moeten het gezag hebben over het kind).
4. Een antwoord of weigering wordt altijd gemotiveerd in begrijpelijke taal.
5. De betrokkene krijgt binnen 4 weken na het indienen van zijn verzoek antwoord. Als dat niet lukt, dan vraagt de school uitstel (van maximaal 4 weken).
6. De betrokkene krijgt alleen inzage in de eigen gegevens. Als er persoonsgegevens van andere betrokkene bij staan, dan haalt de school die informatie weg of schermen die af. Zodra de persoonlijke levenssfeer van derden wordt geraakt, of als het gaat om informatie die door derden vertrouwelijk zijn verstrekt, geeft de school ook geen inzage.
7. Als een dossier wordt ingericht of samengesteld heeft de betrokkene het recht om alles in te zien. Het dossier is zo opgebouwd dat een deskundige, collega of waarnemer de professionele relatie kan voortzetten.
8. Er is één uitzondering op het inzage geven: als het in het belang van de betrokkene is om geen inzage te geven, blijft inzage achterwege, bijvoorbeeld dossiervorming bij verdenking van misbruik of kindermishandeling. Het is in het belang van het kind om de ouders géén inzage te geven. Dit is echter een grote uitzondering waar terughoudend mee om moet worden gegaan.

Persoonlijke aantekeningen en werkaantekeningen

Als er over een betrokkene persoonlijke werkaantekeningen zijn gemaakt, dan maken die geen deel uit van het dossier van de betrokkene. Ze vallen daarmee buiten het inzagerecht. Voorwaarde is wel dat het moet gaan om persoonlijke werkaantekeningen: de aantekeningen zijn niet bedoeld om te delen met collega's, en ze mogen niet toegankelijk zijn voor anderen, bijvoorbeeld geheugensteuntjes, een voorlopig schooladvies of een registratie van een leraar hoe vaak een leerling gewaarschuwd in zijn les. Zodra persoonlijke werkaantekeningen zijn besproken of ingebracht in bijvoorbeeld in een rapportbespreking, zijn het geen persoonlijke aantekeningen meer.
Aantekeningen in het leerling administratiesysteem in het veld 'notities' zijn géén persoonlijke aantekeningen en de betrokkene heeft het recht om die in te zien. Ditzelfde geldt ook voor een personeelsdossier: zodra er meer medewerkers dan alleen een leidinggevende toegang hebben tot aantekeningen, zijn het geen persoonlijke aantekeningen meer.

Bijlage 9: Privacyreglement voor scholen van Stichting ISA

Iedere school verwerkt persoonsgegevens van personeel en leerlingen en/of ouders. In het privacyreglement wordt vast gelegd voor welke doelen je persoonsgegevens registreert. Het gaat hierbij niet alleen om gewone persoonsgegevens zoals naam, geboortedatum en overige contactgegevens, maar soms ook om bijzondere persoonsgegevens met betrekking tot bijvoorbeeld gezondheid, afkomst en godsdienst.
In het privacyreglement zijn in ieder geval alle onderdelen en processtappen beschreven die in bijlage 8 is geregeld. Het bevoegd gezag is verantwoordelijk voor de bescherming van de privacy van leerlingen en/of ouders en medewerkers en stelt dan ook het privacyreglement vast. Het privacyreglement is daarmee voor alle scholen die onder Stichting ISA vallen van toepassing.

Privacyreglement voor scholen van Stichting ISA

1. Aanhef	Dit reglement is voor de scholen die onder Stichting Islamitische School Amsterdam ressorteren, gevestigd te Amsterdam.
2. Definities	
Persoonsgegevens	Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;
Verwerking van persoonsgegevens	Eke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;
Bijzonder persoonsgegeven	Een persoonsgegeven dat iets zegt over iemand zijn godsdienst, levensovertuiging, ras, politieke gezindheid of zijn gezondheid;
Betrokkene	Degene op wie een persoonsgegeven betrekking heeft al dan niet vertegenwoordigd door diens wettelijk vertegenwoordiger. In dit reglement gaat het om de leerlingen en/of ouders en medewerkers**;**
Wettelijk vertegenwoordiger	Indien de betrokkene de leeftijd van zestien jaren nog niet heeft bereikt, wordt de betrokkene vertegenwoordigd door zijn wettelijk vertegenwoordiger. Meestal zal dit een ouder zijn maar het kan hier ook gaan om een voogd;
Verantwoordelijke	De verantwoordelijke stelt vast welke persoonsgegevens er verwerkt worden én wat het doel is van die verwerking. Dat wil zeggen het bevoegd gezag. Wanneer er in dit reglement gesproken wordt over de Verantwoordelijke dan wordt daarmee het bevoegd gezag van de school bedoeld.
Bewerker	Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;
Derde	Ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken;
School	De verantwoordelijke onderwijsinstelling/bevoegd gezag.
3. Reikwijdte en doelstelling	1. Dit reglement stelt regels over de verwerking van persoonsgegevens van leerlingen en of ouders en medewerkers van de school. 2. Dit reglement is van toepassing op alle persoonsgegevens van de betrokkene die door school worden verwerkt. Dit reglement heeft tot doel: a. de persoonlijke levenssfeer van de betrokkenen te beschermen tegen verkeerd en onbedoeld gebruik van de persoonsgegevens; b. vast te stellen welke persoonsgegevens worden verwerkt en met welk doel dit gebeurt; c. de zorgvuldige verwerking van persoonsgegevens te waarborgen; d. de rechten van betrokkene te waarborgen.
4. Doelen van de verwerking van persoonsgegevens	Bij de verwerking van persoonsgegevens houdt de school zich aan de relevante wetgeving waaronder de Wet bescherming persoonsgegevens.
Doelen	De verwerking van persoonsgegevens vindt plaatst voor: a. de organisatie of het geven van het onderwijs, de begeleiding van leerlingen, deelnemers of studenten, dan wel het geven van studieadviezen; b. het verstrekken of ter beschikking stellen van leermiddelen;

	c. het bekend maken van informatie over de school en leermiddelen als bedoeld, onder a en b, alsmede informatie over de leerlingen, deelnemers of studenten, bedoeld in het eerste lid, op de eigen website; d. het bekendmaken van de activiteiten van de school op de eigen website; f. het behandelen van geschillen en het doen uitoefenen van accountantscontrole; g. het onderhouden van contacten met de oud-leerlingen, oud-deelnemers of oud-studenten van de verantwoordelijke; h. de uitvoering of toepassing van een andere wet.
5. Vrijstelling meldingsplicht	De in artikel 4 genoemde gegevensverwerkingen vallen onder het vrijstellingsbesluit Wbp en hoeven niet worden aangemeld bij het CBP.
6. Doelbinding	Persoonsgegevens worden uitsluitend gebruikt voor zover dat gebruik verenigbaar is met de omschreven doelen van de verwerking. De school verwerkt niet meer gegevens dan noodzakelijk is om die vastgestelde doelen te bereiken.
7. Soorten gegevens	De door de school gebruikte categorieën van persoonsgegevens worden in bijlage 1 opgesomd.
8. Grondslag verwerking	Verwerking van persoonsgegevens gebeurt alleen op grond van: a. Toestemming: in het geval de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend b. Overeenkomst: in het geval de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst c. Wettelijke verplichting: in het geval *de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de school onderworpen is* d. Vitaal belang: e. Publiekrechtelijke taak: in het geval de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt f. Gerechtvaardigd belang:
9. Bewaartermijnen	De school bewaart de gegevens niet langer dan dat zij noodzakelijk zijn voor het vervullen van het doel waarvoor zij zijn verkregen, tenzij er een andere wettelijke verplichting is die het langer bewaren van de gegevens verplicht stelt.
10. Toegang	De school verleent slechts toegang tot de in de administratie en systemen van de school opgenomen persoonsgegevens aan: a. de bewerker en de derde die onder rechtstreeks gezag van de school staat; b. de bewerker die gemachtigd is om persoonsgegevens te verwerken;' c. derden die op grond van de wet toegang moet worden verleend, waarbij alleen toegang wordt verleend aan de gegevens waartoe volgens de wet toegang toe moet worden gegeven.
11. Beveiliging en geheimhouding	a. De school neemt passende technische en organisatorische beveiligingsmaatregelen om te voorkomen dat de persoonsgegevens worden beschadigd, verloren gaan of onrechtmatig worden verwerkt. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen. b. De school zorgt dat betrokkenen niet meer inzage of toegang hebben tot de persoonsgegevens dan zij strikt noodzakelijk nodig hebben voor de goede uitoefening van hun werk. c. Bij de beveiligingsmaatregelen wordt rekening gehouden met de stand van de techniek en de kosten van de tenuitvoerlegging. Daarbij houdt de school rekening met de concrete risico's die van toepassing kunnen zijn op de verwerkte persoonsgegevens. d. Iedereen die betrokken is bij de uitvoering van dit reglement, en daarbij de beschikking krijgt over persoonsgegevens die vertrouwelijk zijn of geheim moeten worden gehouden (zoals bijvoorbeeld zorggegevens), en voor wie niet reeds uit hoofde van beroep, functie of wettelijk voorschrift een geheimhoudingsplicht geldt, is verplicht tot geheimhouding van die persoonsgegevens daarvan.
12. Verstrekken gegevens aan derden	Wanneer daartoe een wettelijke plicht bestaat kan school de persoonsgegevens verstrekken aan derden. Het verstrekken van persoonsgegevens aan derden kan ook plaatst vinden na toestemming van de betrokkene.
13. Sociale media	Voor het gebruik van persoonsgegevens in sociale media, zijn aparte afspraken gemaakt in het 'sociale-mediaprotocol' van de school.

14. Rechten betrokkenen	1. De Wbp geeft de betrokkene een aantal rechten. De school erkent deze rechten en handelt in overeenstemming met deze rechten.
Inzage	Elke betrokkene heeft recht op inzage van de door de school verwerkte persoonsgegevens die op hem/haar betrekking hebben. De school kan vragen om een geldig identiteitsbewijs ter verificatie van de identiteit van de verzoeker
Verbetering, aanvulling, verwijdering en afscherming	Betrokkene kan een verzoeken doen tot verbetering, aanvulling, verwijdering of afscherming van zijn persoonsgegevens, tenzij dit onmogelijk blijkt of een onredelijke inspanning zou vergen.
Verzet	Voor zover school persoonsgegevens gebruikt op de grond van artikel 8 onder e en f, dan kan de betrokkene zich verzetten tegen verwerking van persoonsgegevens op basis van diens persoonlijke omstandigheden.
Termijn	2. De school dient binnen een termijn van 4 weken na ontvangst van een verzoek hieraan schriftelijk gehoor te geven dan wel deze schriftelijk, gemotiveerd af te wijzen. De school kan de betrokkene laten weten dat er meer tijd nodig en deze termijn verlengen met maximaal 4 weken.
Uitvoeren verzoek	3. Indien het verzoek van de betrokkene wordt gehonoreerd, draagt de school zorg voor het zo spoedig mogelijk doorvoeren van de verzochte wijzigingen.
Intrekken toestemming	4. Voor zover voor de verwerking van persoonsgegevens voorafgaande toestemming vereist is, kan deze toestemming ten allen tijden door de wettelijk vertegenwoordiger worden ingetrokken.
15. Transparantie	1. De school informeert de betrokkene over de verwerking van zijn persoonsgegevens. Indien het type verwerking dat vraagt, informeert de school iedere betrokkene apart over de details van die verwerking. 2. De school informeert de betrokkene – op hoofdlijnen – ook over de afspraken die gemaakt zijn met derden en bewerkers die persoonsgegevens van de betrokkene ontvangen.
16. Klachten	1. Wanneer de betrokkene van mening is dat het doen of nalaten van de school niet in overeenstemming is met de Wbp of zoals dat is uitgewerkt in dit reglement is, dan dient hij/zij zich te wenden tot **directeur-bestuurder** van de school. 2. Overeenkomstig de Wpb kan de betrokkene zich eveneens wenden tot de rechter of het College Bescherming Persoonsgegevens.
17. Onvoorziene situatie	Indien er zich een situatie voordoet die niet beschreven is in dit reglement dan neemt de verantwoordelijke de benodigde maatregelen.
18. Wijzigingen reglement	1. Dit reglement wordt na instemming van de (G)MR vastgesteld door de verantwoordelijke. De verantwoordelijke maakt dit reglement openbaar via **website en beleidsdocumenten**. De verantwoordelijke heeft het recht dit reglement, na instemming van de (G)MR te wijzigingen.
19. Slotbepaling	Dit reglement wordt aangehaald als “het privacyreglement” van de school en treed in werking op **[DATUM].**

Bijlage bij Privacyreglement: Overzicht van categorieën gebruikte persoonsgegevens

Omschrijving en opsomming categorieën persoonsgegevens die gebruikt worden:
Als school hebben wij diverse persoonsgegevens van leerlingen en hun wettelijk vertegenwoordigers nodig om te kunnen voldoen aan onze verplichtingen, om op een goede manier onderwijs te kunnen geven en om invulling te geven aan diverse andere doeleinden (die verderop in deze privacyreglement zijn opgesomd).
Bijvoorbeeld:
a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie bedoelde gegevens van de betrokkene;
b. het persoonsgebonden nummer (BSN);
c. nationaliteit en geboorteplaats;
d. gegevens als bedoeld onder a, van de wettelijk vertegenwoordiger of verzorger van de leerling;
e. gegevens betreffende de gezondheid of het welzijn van de leerling voor zover die noodzakelijk zijn voor de ondersteuning;
f. gegevens betreffende de godsdienst of levensovertuiging van de leerling, voor zover die noodzakelijk zijn voor de school, het onderwijs of de te geven ondersteuning;
g. gegevens betreffende de aard en het verloop van het onderwijs en ondersteuning, alsmede de behaalde studieresultaten;
h. schoolgegevens (waaronder naam school, naam zorgcoördinator/mentor/ intern begeleider, klas/groep waarin de leerling zit, tijdstip van inschrijving bij deze school, naam van de indiener van de aanmelding bij het samenwerkingsverband, schoolloopbaan en rapportage vanuit primair en voortgezet onderwijs);

i. aanleiding voor de aanmelding bij het samenwerkingsverband, relevante screenings- en onderzoeksgegevens en omschrijving van de problematiek die aan de orde is;
j. activiteiten die door de school zijn ondernomen rond de betreffende leerling, alsmede de resultaten hiervan;
k. bestaande of (relevante) afgesloten hulpverleningscontacten en de namen van contactpersonen;
l. relevante persoonsgegevens die door externe partijen worden verstrekt met betrekking tot de aangemelde problematiek van de betreffende leerling;
m. relevante financiële gegevens;

Sommige door ons verwerkte persoonsgegevens zijn bijzondere persoonsgegevens. Bijvoorbeeld gezondheidsgegevens die noodzakelijk zijn voor het adequaat ondersteunen van een leerling. Deze persoonsgegevens mogen alleen onder specifieke voorwaarden worden verwerkt. Dat betekent dat wij deze persoonsgegevens alleen verwerken als aan deze voorwaarden voldaan is. Sommige persoonsgegevens zijn voor ons zodanig noodzakelijk dat wij, gelet op de doelstellingen van onze organisatie en vanwege de op ons rustende wettelijke verplichtingen, niet zonder kunnen. Wij hebben bijvoorbeeld diverse gegevens van de leerling en zijn wettelijke vertegenwoordiger(s) nodig voor de beoordeling van de aanmelding en het verrichten van de inschrijving. Als dergelijke gegevens niet worden verstrekt, kunnen wij de aanmelding niet beoordelen en de leerling dus ook niet inschrijven

Soms verstrekken wij ook persoonsgegevens aan andere organisaties. Dat moet dan wel passen bij onze doeleinden en er moet een wettelijke grondslag voor bestaan (zie hierboven). In de eerste plaats zijn er leveranciers die op onze instructie persoonsgegevens verwerken. Denk aan de leveranciers van het administratie- en/of leerlingvolgsysteem en van (al dan niet) digitale leermiddelen. Met dergelijke leveranciers (‘verwerkers’) zijn goede afspraken gemaakt om de betreffende persoonsgegevens te beschermen en te beveiligen. We zullen persoonsgegevens van leerlingen en hun wettelijk vertegenwoordigers niet delen met commerciële derde partijen voor andere doeleinden.

De school bewaart persoonsgegevens niet langer dan noodzakelijk is voor het doel waarvoor de persoonsgegevens worden verwerkt. De meeste gegevens uit het leerling dossier bewaren wij gedurende (maximaal) twee jaar nadat de leerling is uitgeschreven bij onze school; voor sommige gegevens geldt een langere (wettelijke) bewaartermijn. Indien u hierover vragen heeft, kunt u contact opnemen met de FG van de school.

U heeft de volgende rechten:
- uitleg krijgen over welke persoonsgegevens wij van u hebben en wat we daarmee doen;
- inzage in deze persoonsgegevens;
- het laten corrigeren van fouten;
- het laten verwijderen van (bijvoorbeeld) verouderde persoonsgegevens;
- intrekken van toestemming voor het verwerken van persoonsgegevens, als de verwerking berust op deze toestemming;
- bezwaar maken tegen gebruik van persoonsgegevens, met name als u vindt dat wij onvoldoende belang hebben bij het verwerken van de gegevens;
- het laten beperken van de verwerking van persoonsgegevens, indien u een verzoek heeft gedaan tot correctie, bezwaar heeft gemaakt of van mening bent dat wij uw persoonsgegevens onrechtmatig verwerken.

Voorts heeft u het recht om ons te verzoeken om persoonsgegevens over te dragen aan een andere organisatie, en om niet te worden onderworpen aan geautomatiseerde besluitvorming. (Voor leerling jonger dan 16 jaar worden deze rechten uitgeoefend door hun wettelijk vertegenwoordigers.)
Om een beroep te doen op de bovenstaande rechten, kunt u zich schriftelijk (per e-mail: helpdesk@as-siddieq.nl) wenden tot de FG. Vervolgens wordt beoordeeld in hoeverre aan uw verzoek kan worden voldaan. Daarbij houden wij ons aan de wettelijke voorschriften.

Bijlage 10: Geheimhouding overeenkomst voor de scholen van Stichting ISA

Richting vaste medewerkers worden de afspraken rondom de bescherming van persoonsgegevens vaak als onderdeel van de arbeidsovereenkomst vastgelegd. Voor minder vaste medewerkers, stagiaires en ingehuurd personeel worden deze afspraken niet opgenomen in de contracten. In dat geval maakt de school gebruik van een geheimhoudingsverklaring.

Handleiding bij gebruik:

Deze geheimhoudingsovereenkomst is bedoeld voor "externen": stagiaires (va. 16 jr; jonger dan 16 moeten de ouders tekenen), vrijwilligers, ZZP'ers, leveranciers enz.

Geheimhouding voor medewerkers van de onderwijsinstelling (dus echt de mensen die in loondienst zijn van de onderwijsorganisatie) vloeit deels voort uit de wet en kan geregeld worden in de arbeidsovereenkomst.

Geheimhoudingsovereenkomst voor de scholen van Stichting ISA

Naam …….

Datum ……

Referentie …….

Ondergetekenden:

Stichting Islamitische School Amsterdam, gevestigd en kantoorhoudende aan de Jan van Riebeekstraat 11-13 1057 ZW Amsterdam hierbij vertegenwoordigd door de R.Boudil, directeur-bestuurder, hierna te noemen: "Onderwijsinstelling",

En

De heer / mevrouw …… werkzaam bij IBS Al Maes/Al Jawhara/Al Yaqoet in de functie van ……. hierna te noemen: " ……..",

Hierna samen te noemen: "Partijen",

Partijen overwegende dat:

1. Onderwijsinstelling IBS Al Maes/Al Jawhara/Al Yaqoet verzorgt onderwijs aan kinderen tussen 2,5 tot 12 jaar;
2. Onderwijsinstelling IBS Al Maes/Al Jawhara/Al Yaqoet een overeenkomst heeft gesloten voor onderwerp overeenkomst;
3. Naam werkzaamheden in het kader van deze overeenkomst zal uitoefenen, waarbij hij/zij toegang krijgt tot Vertrouwelijke informatie die toebehoort aan de Onderwijsinstelling of die aan de Onderwijsinstelling is toevertrouwd;
4. Deze geheimhoudingsovereenkomst geldt als aanvulling op de overeenkomst met referentienummer [NUMMER]
5. Partijen met deze geheimhoudingovereenkomst het gebruik van vertrouwelijke informatie beogen te regelen;

De partijen verklaren als volgt te zijn overeengekomen:

In deze geheimhoudingsovereenkomst worden de volgende nader te omschrijven begrippen aangeduid met een hoofdletter:

1. Overeenkomst: de overeenkomst met referentienummer [NUMMER] d.d. [DATUM]
2. Geheimhoudingsovereenkomst: deze geheimhoudingsovereenkomst
3. Vertrouwelijke informatie: informatie waarvan Naam weet of behoort te weten dat het Vertrouwelijke informatie betreft of informatie die aangeduid is al Vertrouwelijke informatie.
4. **Voorwerp van deze overeenkomst**
   1. [Naam] zal de werkzaamheden verrichten zoals beschreven in de Overeenkomst.
   2. In het kader van de Overeenkomst zal Naam toegang krijgen tot Vertrouwelijke informatie, die toebehoort aan de Onderwijsinstelling of die aan de Onderwijsinstelling is toevertrouwd, zoals maar niet beperkt tot: omschrijving vertrouwelijke info waartoe de ingezette persoon toegang krijgt.
   3. [Naam] legt de verplichtingen zoals omschreven in de Geheimhoudingsovereenkomst onverkort op aan personeel of derden waarvan hij zich bedient.

5. **Geheimhouding**
   1. [Naam] zal geheimhouding betrachten ten aanzien van alle Vertrouwelijke informatie die in het kader van de werkzaamheden voor de Onderwijsinstelling tot zijn beschikking komt.

   Dit geldt niet voor informatie die:

- algemene bekend is,
- voorheen al bekend was,
- door een derde te goeder trouw ter beschikking is gesteld, waarvan wettelijke voorschriften vereisen, dat deze bekend gemaakt moet worden.

   2. Onder geheimhouding wordt tevens verstaan dat [Naam] de verkregen Vertrouwelijke informatie niet voor eigen doeleinden mag gebruiken.
   3. [Naam] verplicht zich bij de uitvoering van zijn/haar werkzaamheden de bepalingen van de gedragscode/handvest van de Onderwijsinstelling (die te vinden is op https://www.invullen) in acht te nemen.
   4. Het is [Naam] niet toegestaan om documenten en andere gegevensdragers, zoals tekeningen, schema´s en andere informatie te vermenigvuldigen zonder de schriftelijke toestemming van de Onderwijsinstelling, en dan slechts ter uitvoering van de Overeenkomst.
   5. Het is [Naam] niet toegestaan om zonder instemming van de Onderwijsinstelling publiciteit te geven aan uitvoering van deze Overeenkomst.
   6. Voor de Onderwijsinstelling ontwikkelde producten, c.q. tot stand gebrachte diensten mogen niet aan derden worden aangeboden, indien deze specifiek voor de Onderwijsinstelling zijn ontwikkeld en het aanbieden aan derden de positie van de Onderwijsinstelling zou schaden.

3. **IBP**
   1. Indien [Naam] toegang krijgt tot de bedrijfsmiddelen (waaronder, maar niet beperkt tot: systemen, hardware(componenten) en informatie) van Onderwijsinstelling, vergewist [Naam] zich van het geldende IBP beleid en procedure voor het aanvaardbaar gebruik van bedrijfsmiddelen van Onderwijsinstelling welke op het eerste verzoek wordt toegestuurd. Het verzoek kan gericht worden aan info@as-siddieq.nl
   2. Indien [Naam] zijn eigen hardware componenten inzet bij de uitvoering van de Overeenkomst treft [Naam] passende beveiligingsmaatregelen volgens het geldende IBP beleid van Onderwijsinstelling conform lid 1 van dit artikel of in afwezigheid daarvan handelt [Naam] in overeenstemming met de normen van informatiebeveiliging ISO 27001 en ISO 27002.

4. **Termijnen**
   1. De Geheimhoudingsovereenkomst gaat in op ingangsdatum overeenkomst en heeft een looptijd van 10 jaar na de beëindiging van de Overeenkomst.

2. Partijen kunnen de Geheimhoudingsovereenkomst schriftelijk onder nader overeen te komen voorwaarden aanpassen en/of verlengen. Deze overeen te komen wijzigingen worden onderdeel van de Geheimhoudingsovereenkomst.

5. **Algemeen**
   1. Op de Geheimhoudingsovereenkomst is Nederlands recht van toepassing. Partijen worden geacht ter zake van deze Overeenkomst domicilie te hebben gekozen te vestigingsplaats Onderwijsinstelling.
   2. Partijen verbinden zich in te spannen om eventuele geschillen in der minne te schikken. Bij gebreke van een minnelijke schikking zullen geschillen die voortvloeien uit de overeenkomst worden voorgelegd aan de bevoegde rechter te [plaatsnaam].

Aldus overeengekomen, in tweevoud opgemaakt en ondertekend,

Namens onderwijsinstelling	Naam wederpartij
Naam:	Naam:
Functie:	Functie:
Datum:	Datum:

Bijlage 11: Transparantie over Privacy stichting ISA

Algemeen

Op IBS Al Maes/ASl Jawhara/Al Yaqoet wordt zorgvuldig omgegaan met de privacy van de leerlingen. De school heeft leerlinggegevens nodig om leerlingen goed onderwijs te kunnen geven en te begeleiden. Ook worden de gegevens opgeslagen voor de goede administratieve organisatie van de school. De meeste leerlinggegevens komen van ouders (zoals bij de inschrijving op school), maar ook leraren en ondersteunend personeel leggen gegevens vast over de leerlingen (bijvoorbeeld cijfers en vorderingen). Soms worden er bijzondere persoonsgegevens, zoals medische informatie (dyslexie of ADHD), geregistreerd als dat nodig voor de juiste begeleiding van een leerling.

Tijdens de lessen wordt gebruik gemaakt van een aantal digitale leermaterialen. Hiervoor is een beperkte set met persoonsgegevens nodig om bijvoorbeeld een leerling te identificeren. Met de leveranciers van deze leermiddelen zijn duidelijke afspraken gemaakt over het gebruik van de gegevens die ze van de school krijgen. Een leverancier mag de leerlinggegevens alleen gebruiken als de school daar toestemming voor geeft.

De leerlinggegevens worden opgeslagen in ons (digitale) administratiesysteem Parnassys. De vorderingen van de leerlingen worden vastgelegd in ons leerlingvolgsysteem Parnassys. Dit programma is beveiligd en toegang tot die gegevens is beperkt tot medewerkers van onze school. Omdat de school onderdeel uitmaakt van Stichting ISA worden daar ook (een beperkt aantal) persoonsgegevens mee gedeeld in het kader van de gemeenschappelijke administratie en het plaatsingsbeleid.

Ouders hebben het recht om de gegevens van en over hun kind(eren) in te zien. Als de gegevens niet kloppen, moet de informatie gecorrigeerd worden. Als de gegevens die zijn opgeslagen niet meer relevant zijn voor de school, vraagt de school de betrokkenen die specifieke gegevens te laten verwijderen. Voor vragen of het uitoefenen van de rechten van de betrokkene, kun hij/zij contact opnemen met de leraar/lerares van het kind, of met de schooldirecteur (zie bijlage 7: *Rechten van betrokkenen Stichting ISA*).

In het privacyreglement is beschreven hoe de school omgaat met haar leerlinggegevens, en wat de rechten zijn van ouders en leerlingen. Meer informatie over privacy is op de website van de school te lezen.

Voor het gebruik van foto’s en video-opnames van leerlingen op bijvoorbeeld de website van de school of in de nieuwsbrief, vragen wij altijd vooraf toestemming van de ouders/verzorgers. Ouders mogen altijd besluiten om die toestemming niet te geven, of om eerder gegeven instemming in te trekken. Als de ouders/verzorgers toestemming hebben gegeven, blijven wij natuurlijk zorgvuldig met de foto’s omgaan en wegen wij per keer af of het verstandig is een foto te plaatsen.

Basispoort

Om leerlingen eenvoudig toegang te geven tot digitaal leermateriaal van de school, maakt de school gebruik van Basispoort. Deze software maakt het geven van onderwijs op maat via gedigitaliseerde leermiddelen mogelijk. Het maken van bijvoorbeeld een online toets is alleen mogelijk als de leerkracht weet welke leerling de antwoorden heeft ingevoerd. Hiervoor zijn leerlinggegevens nodig. De school heeft met Basispoort een overeenkomst gesloten waarin afspraken zijn gemaakt over het gebruik van de leerlinggegevens. Basispoort maakt voor het schooljaar 2018/2019 gebruik van de volgende set met gegevens: een identificatienummer van Basispoort, voornaam, achternaam, tussenvoegsel, geboortedatum, leerlingkey, groepskey, groepsnaam, jaargroep, geslacht en het identificatienummer van de school. Via Basispoort worden er dus geen leer- of toets resultaten opgeslagen en/of uitgewisseld.

Inschrijfformulier

Op de website van de school staat het inschrijfformulier van de school. De ouders/verzorgers ontvangen een bevestiging van de inschrijving.

De meeste vragen op het formulier spreken voor zich. Een aantal vragen zijn wij wettelijk verplicht aan ouders/verzorgers te stellen. Zo vragen wij naar het opleidingsniveau. Dit heeft te maken met de wettelijke ‘gewichtenregeling’: het aantal leerkrachten aan onze school is mede afhankelijk van het totaal van het

‘leerlingengewicht’ van onze leerlingen. (Na schooljaar 2019-2020 zal de gewichtenregeling vervangen worden door schoolgewicht.)

De gegevens die ouders/verzorgers hebben ingevuld op het inschrijfformulier, worden opgeslagen in de leerlingenadministratie van de school. Uiteraard worden deze gegevens vertrouwelijk behandeld. Op de administratie is de Wet bescherming persoonsgegevens van toepassing. Dit betekent onder andere dat de gegevens door de school worden beveiligd, en dat de toegang tot de administratie is beperkt tot alleen personeel die de gegevens strikt noodzakelijk nodig heeft. Ouders/verzorgers hebben het recht om de door de school geregistreerde gegevens in te zien (voor zover die informatie betrekking heeft op het kind). Als de gegevens niet kloppen, dan mogen ouders/verzorgers van de school verwachten dat zij – op verzoek - de informatie verbeteren of aanvullen.

Telefoonlijst
Op de school wordt er, per klas, een klassenlijst gemaakt met de adressen van leerlingen. Deze lijst met contactgegevens is erg praktisch om te overleggen met andere ouders, als de kinderen (buiten schooltijd) willen afspreken of als er vragen zijn rondom school, overblijf of bijvoorbeeld huiswerk. De school vraagt toestemming van ouders/verzorgers om de naam van het kind, diens adres en uw telefoonnummer te mogen delen met de andere (ouders van de) klasgenootjes van het kind. Als er bezwaar tegen is, wordt de naam van het kind niet gedeeld (en moeten ouders/verzorgers daar zelf voor zorgen). Deze informatie op de klassenlijst wordt uitsluitend gebruikt voor persoonlijk gebruik onderling, en dus niet voor bijvoorbeeld reclame.

Bijlage 12: Wachtwoord beleid

Veel applicaties die in het PO gebruikt worden zijn online. Leerlingen moeten allemaal inloggen met een gebruikersnaam en een wachtwoord. Hoe gaan we als school nu mee om en hoe houden we dat praktisch uitvoerbaar?

Hoe moet het niet?

We kiezen niet voor één simpel wachtwoord voor elke leerling om veel 'gedoe' te voorkomen.

De zorg zit niet zo zeer in het feit dat leerlingen onderling bij elkaar kunnen kijken, maar meer in de onveiligheid en risico's naar buiten toe. Uit de programma's kunnen veel gegevens afgeleid worden, totaalscores, gesprekken via de chat enz.

Als het gaat om digitale vaardigheden en IBP, dan spreekt het vanzelf dat we leerlingen zo vroeg mogelijk leren om zorgvuldig om te gaan met hun persoonsgegevens en dus ook met hun wachtwoorden. Dit sluit aan bij het mediawijs maken van leerlingen en de *ICT-basisvaardigheden.* En dat leren we ze niet door ze allemaal hetzelfde wachtwoord te geven...

Hoe gaan we dat nu aanpakken?

De drie basisregels voor wachtwoorden zijn voor iedereen gelijk. Ook jonge kinderen moeten we deze aanleren:

1. **Je wachtwoord mag je nooit delen, dat is iets van jou.**
2. **Je wachtwoord mag niet makkelijk te raden zijn**
3. **Je wachtwoord mag je niet hergebruiken. Gebruik voor alles een eigen wachtwoord.**

De *eerste regel* sluit dus uit dat wachtwoorden voor alle kinderen hetzelfde zijn. Een wachtwoord is persoonlijk.

De *tweede regel* heeft te maken met complexiteit. Hier wordt het wat lastiger, want kinderen moeten het wel kunnen onthouden. Mensen mogen je wachtwoord niet kunnen raden, maar ook computers niet.

- Mensen kunnen je wachtwoord makkelijk raden wanneer je iets heel simpels of bekends gebruikt, zoals de naam van je hond.
- Computers kunnen je wachtwoord makkelijk raden wanneer het kort is.

Vroeger werden korte, maar complexe wachtwoorden aanbevolen. Deze zijn voor een mens moeilijk te raden (maar wel te onthouden). Echter de huidige snellere computers kunnen deze wachtwoorden wél snel achterhalen. Een lang wachtwoord of een 'wachtzin' is dan ook beter dan een kort complex wachtwoord.

De *derde regel* is voor jonge kinderen (PO) niet realistisch.

Bijlage 13: Responsible Disclosure

Voor de school speelt ict een steeds grotere rol in de ondersteuning van het onderwijs. Het is de verantwoordelijkheid van de school om te zorgen dat het onderwijs altijd door kan gaan en dat de veiligheid van een informatiesysteem en (software)producten wordt gegarandeerd.
Ondanks alle aandacht voor de beveiliging van systemen kan het voorkomen dat er toch een zwakke plek, een kwetsbaarheid, is. Als iemand een zwakke plek in één van de systemen heeft gevonden dan treft de school zo snel mogelijk de juiste maatregelen.
Ook al worden kwetsbaarheden zonder kwade bedoelingen bij toeval ontdekt, vaak worden ze niet gemeld bij de school. Wanneer de school beveiligingsproblemen duidelijk naar buiten communiceert, weten medewerkers en leerlingen beter waar ze aan toe zijn wanneer ze een kwetsbaarheid willen melden. Dit voorkomt onzekerheid en paniek aan beide kanten en beperkt eventuele schade zoveel mogelijk.
Het **responsible disclosure** beleid heeft als doel om de drempel tot het melden van deze kwetsbaarheden te verlagen, waardoor het beveiligingsniveau van informatiesystemen en het netwerk verhoogt kan worden en schade voor de schoolbestuurder kan worden beperkt en/of voorkomen. Het responsible disclosure beleid is een oplossing om op een maatschappelijk verantwoorde en effectieve manier om te gaan met het melden van ict-kwetsbaarheden. Het geeft de mogelijkheid om af te spreken dat bij eventueel strafrechtelijk handelen van de melder geen aangifte zal worden gedaan of civielrechtelijke stappen zullen worden ondernomen.
Voor zowel de school als voor de melder schept het beleid duidelijkheid in de verantwoordelijkheden die beide partijen hebben. Het aanbieden van een beloning kan leerlingen mogelijk (extra) motiveren om een kwetsbaarheid te melden.

Responsible Disclosure voor leerlingen van scholen van Stichting ISA

Bij Stichting ISA vinden wij de veiligheid van onze informatiesystemen (internet en bijbehorende hardware en software) erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek (kwetsbaarheid) is. Als jij een zwakke plek in één van onze systemen hebt gevonden, dan horen wij dit graag, zodat we zo snel mogelijk maatregelen kunnen treffen. Wij willen graag met jou samenwerken om de leerlingen, medewerkers en onze systemen beter te kunnen beschermen.

Wij vragen jou:

- Je bevindingen te mailen naar ***helpdesk@as-siddieq.nl*** of deze door te geven aan je leerkracht. Jouw leerkracht zal vervolgens in contact treden met onze security officer;
- De kwetsbaarheid niet te misbruiken door bijvoorbeeld meer informatie te downloaden dan nodig is om het lek aan te tonen of informatie van andere leerlingen, docenten of andere medewerkers in te kijken, te verwijderen of aan te passen;
- De kwetsbaarheid niet met anderen te delen totdat deze is verholpen en alle informatie die verkregen is via het lek direct na het verhelpen van het lek te wissen;
- Geen gebruik te maken van aanvallen op de beveiliging van de school;
- De school voldoende informatie te geven om het probleem te kunnen vinden zodat wij het zo snel mogelijk kunnen verhelpen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij meer ingewikkelde kwetsbaarheden kan extra informatie nodig zijn.

Wij beloven dat:

- Je binnen 3 dagen van ons te horen krijgt hoe we de kwetsbaarheid gaan oppakken en wanneer wij hiervoor een oplossing verwachten te hebben;
- Als je de kwetsbaarheid netjes gemeld hebt en via de bovenstaande stappen gehandeld hebt, zullen wij geen melding maken bij de politie*;
- Wij jouw melding vertrouwelijk behandelen en dat jouw persoonlijke gegevens niet zonder jouw toestemming met anderen delen worden tenzij dit wettelijke verplicht is;
- Wij je op de hoogte houden van de voortgang van het verhelpen van de kwetsbaarheid.

* Let op: ons beleid voor responsible disclosure is geen uitnodiging om ons netwerk uitgebreid te scannen om zwakke plekken te ontdekken. Er bestaat een kans dat je tijdens jouw ‘zoektocht’ handelingen uitvoert die

strafbaar zijn. Het feit dat Stichting ISA geen aangifte tegen je zal doen sluit niet uit dat er een strafrechtelijk onderzoek naar jouw handelen gehouden kan worden dan wel dat je strafrechtelijk kunt worden veroordeeld.

Responsible Disclosure voor medewerkers van scholen van Stichting ISA

Bij Stichting ISA vinden wij de veiligheid van onze systemen erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek is. Als u een zwakke plek in één van onze systemen heeft gevonden, dan horen wij dit graag, zodat we zo snel mogelijk maatregelen kunnen treffen. Wij willen graag met u samenwerken om onze gebruikers en onze systemen beter te kunnen beschermen.

Wij vragen u:

- Uw bevindingen te mailen naar ***helpdesk@as-siddieq.nl*** of telefonisch contact op te nemen met onze security office;
- De kwetsbaarheid niet te misbruiken door bijvoorbeeld meer data te downloaden dan nodig is om het lek aan te tonen of (persoons)gegevens van derden in te kijken, te verwijderen of aan te passen;
- De kwetsbaarheid niet met anderen te delen totdat deze is verholpen en alle (vertrouwelijke) gegevens die zijn verkregen via de lek direct na het verhelpen van de lek te wissen;
- Geen gebruik te maken van aanvallen op fysieke beveiliging, social engineering, distributed denial of service, spam of applicaties van derden;
- Voldoende informatie te geven om het probleem te reproduceren zodat wij het zo snel mogelijk kunnen verhelpen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere kwetsbaarheden kan meer nodig zijn.

Wij zeggen toe dat:

- Wij reageren binnen 3 dagen op uw melding met onze beoordeling van de melding en een verwachte datum voor een oplossing;
- Als u zich aan bovenstaande voorwaarden heeft gehouden zullen wij geen juridische stappen tegen u ondernemen met betrekking tot de melding*;
- Wij behandelen uw melding vertrouwelijk en zullen uw persoonlijke gegevens niet zonder uw toestemming met derden delen tenzij dat noodzakelijk is om een wettelijke verplichting na te komen. Melden onder een pseudoniem is mogelijk;
- Wij houden u op de hoogte van de voortgang van het verhelpen van de kwetsbaarheid;
- In berichtgeving over het gemelde probleem zullen wij, indien u dit wenst, uw naam vermelden als de ontdekker. Wij streven ernaar om alle problemen zo snel mogelijk op te lossen en wij worden graag betrokken bij een eventuele publicatie over het probleem nadat het is opgelost.

* Let op: ons beleid voor responsible disclosure is geen uitnodiging om ons netwerk uitgebreid te scannen om zwakke plekken te ontdekken. Er bestaat een kans dat u tijdens uw onderzoek handeling uitvoert die volgens het strafrecht strafbaar zijn. Het feit dat Stichting ISA geen aangifte tegen u zal doen sluit niet uit dat er een strafrechtelijk onderzoek naar uw handelen gehouden kan worden dan wel dat u strafrechtelijk kunt worden veroordeeld.

Bijlage 14: Bewerkersovereenkomst

Afspraken met leveranciers: Bewerkersovereenkomsten
In het IBP-beleid is al aangegeven dat de school verantwoordelijk is voor de zorgvuldige omgang met de persoonsgegevens van leerlingen. Om dit te kunnen garanderen zijn goede afspraken met aanbieders van digitale leermiddelen van belang.

Bewerkersovereenkomst
Dankzij het convenant '**Digitale Onderwijsmiddelen en Privacy 2.0**' is het voor scholen eenvoudiger om afspraken te maken met leveranciers. Belangrijkste punt in het convenant is de rolverdeling: scholen hebben de regie op wat er gebeurt met de persoonsgegevens. Dit mag niet overgelaten worden aan een leverancier (een verwerker). De school beslist wat de leverancier wél en niet met de gegevens mag doen.
Voor een groot deel is het convenant een vertaling van eisen uit privacywetgeving naar de onderwijspraktijk. Het convenant gaat niet alleen over het gebruik van digitaal leermateriaal, maar ook over school- en leerling administratiesystemen zoals ParnasSys.

Bijlagen bij de bewerkersovereenkomst
Bij het convenant hoort een model bewerkersovereenkomst waarmee de school (de verwerkingsverantwoordelijke) de juiste afspraken maakt met leveranciers. Er is afgesproken met vertegenwoordigers van de leveranciers, dat de tekst van het model zo belangrijk is, dat het niet de bedoeling is om het model te wijzigen. Als dat echt noodzakelijk is, moet de leverancier dat in een *aparte* bijlage uitleggen.
Bij de modelbewerkersovereenkomst horen 2 bijlagen. In de **privacy bijsluiter** wordt uitgelegd wat het product van de leverancier doet, welke gegevens er worden uitgewisseld met de leverancier, wat het doel is van die uitwisseling en of de leverancier andere bedrijven inschakelt (dit noemen we subbewerkers). De tweede bijlage is de beschrijving van de **technische en organisatorische beveiligingsmaatregelen** die zijn genomen. Daarin staat bijvoorbeeld wat de afspraken zijn in geval van een beveiligingsincident zoals een datalek.

Aandachtspunten gebruik digitale onderwijsmiddelen
De onderstaande checklist, die gebruikt wordt bij digitale onderwijsmiddelen, laat in een aantal stappen zien waar de school rekening mee moet houden bij het inzetten van digitaal lesmateriaal en wat ze eventueel moet regelen met de leveranciers ervan. (zie pdf bestand '*Checklist gebruik digitale onderwijsmiddelen …*)
Als een leverancier het convenant niet heeft ondertekend is het extra belangrijk om de privacy afspraken goed vast te leggen. Het pdf bestand *'Checklist afspraken leveranciers'* bevat de onderwerpen die De Autoriteit Persoonsgegevens benoemt om in een schriftelijke overeenkomst tussen verwerkingsverantwoordelijke en verwerker vast te leggen.

Certificeringsschema; een veilige en betrouwbare onderwijsketen
Het is voor de school lastig om eenvoudig vast te stellen of een leverancier de juiste beveiligingsmaatregelen heeft genomen. Omgekeerd is het voor leveranciers niet eenvoudig om aan te tonen dat zij tenminste aan de minimale eisen voldoen. Het hanteren van een eenduidige meetlat lost dit probleem op.
Digitale leermiddelen en (administratie)systemen moeten soepel werken en in navolging van de AVG moeten de gegevens, die hierbij verwerkt worden, betrouwbaar en goed beveiligd zijn. Het **certificeringsschema voor informatiebeveiliging** is die meetlat, het is de standaard die hiervoor is ontwikkeld.
Dit certificeringsschema is enerzijds bedoeld voor leveranciers van ict-toepassingen in de onderwijsketen. Zij kunnen op een eenduidige manier aantoonbaar maken dat ze de IBPvan hun diensten en producten op orde hebben.
Anderzijds is het certificeringsschema bedoeld voor onderwijsinstellingen. Bij het specificeren van informatiebeveiligingseisen kun je eenvoudig verwijzen naar het certificeringsschema, in plaats van specifieke eisen te stellen met betrekking tot (veelal technische) maatregelen. Je kan als school met het toetsingskader eenvoudiger (laten) toetsen of de leverancier hun informatiebeveiliging op orde heeft. Vraag aan de leverancier of zij hun dienst hebben beoordeeld met het certificeringsschema en of ze een rapportage kunnen overleggen. Hoe meer scholen dit vragen van hun leveranciers, hoe meer leveranciers het ook als standaard zullen gaan zien. Op deze manier kunnen we samen de beveiliging in de hele keten naar een hoger niveau brengen. Kijk voor meer informatie over het certificeringsschema bij Edu-K.

Bijlage 15: Gebruik beeldmateriaal leerlingen

Het gebruiken van beeldmateriaal, het delen van foto's en video's van leerlingen door scholen, vormt zelden een probleem en is meestal goedbedoeld. Toch eist de wetgever dat de school vooraf toestemming vraagt aan ouders/verzorgers voor het gebruik van beeldmateriaal van leerlingen, als de leerling jonger is dan 16 jaar. Zonder die toestemming mag de school geen foto's en video's van leerlingen gebruiken.
Bij het vragen van toestemming zijn drie punten van belang:

- De toestemming moet **in vrijheid** gegeven worden; toestemming moet geweigerd kunnen worden zonder dat leerlingen daardoor benadeeld zouden worden.
- De toestemming moet **'ondubbelzinnig'** zijn. Toestemming mag niet verborgen zijn in schoolregels en er mag niet van uitgegaan worden dat ouders toestemming geven als zij niet reageren. Ouders/verzorgers moeten **expliciet** kunnen aangeven waar ze wel of geen toestemming voor verlenen. De school moet de toestemming altijd kunnen aantonen.
- De toestemming moet **specifiek** zijn. Het moet duidelijk zijn waar toestemming voor gegeven wordt en met welk doel. De school zorgt voor **gelaagde** toestemming: wil je toestemming voor foto's op de website, in de schoolgids, nieuwsbrief of in sociale media? De keuze moet duidelijk aan te geven zijn, bijvoorbeeld door een kruisje in een vakje te zetten bij bepaalde type media (foto's/film) of bij bepaalde uitingen (website, schoolkrant, etc.).
  De school maakt vóóraf de juiste afspraken en iedereen weet ook wat die afspraken zijn.

Onderstaande voorbeeld brief wordt gebruikt om toestemming te regelen.

Foto's veilig delen

Naast toestemming vragen is de school ook verantwoordelijk voor het **veilig delen** van beeldmateriaal. Een openbaar fotoalbum mag niet meer. De foto's worden op een beveiligde site geplaatst waarbij ouders moeten inloggen. Hier zijn alléén de foto's van kinderen waarvan de ouders toestemming hebben gegeven om foto's te delen.

Filmen/fotograferen door ouders

Het aantal ouders dat met camera's en smartphones foto's maakt of filmt op school is in de afgelopen jaren flink toegenomen. Ook deze foto's komen al snel op Facebook of YouTube. En wat als een ouder de foto van de beveiligde site kopieert en zelf deelt?
Ook hier geldt dat de school voor álle kinderen een veilige omgeving moet zijn, en niet een plek waar zij (en hun ouders) het risico lopen ongewenst gefotografeerd te worden. Maar het maken van foto's en video's door ouders op school kunnen we moeilijk verbieden. En als een ouder de foto kopieert en zelf deelt neemt de ouder daar de verantwoordelijkheid voor: de school kan niet verbieden dat ouders die foto's overnemen en verder delen (zelfs niet als dat bijvoorbeeld publiek op Facebook is)... De school maakt er wel **afspraken** over, want de school is niet zomaar een openbare plaats waar iedereen toegang toe krijgt.

Toestemming gebruik beeldmateriaal

[Plaats], [maand] [jaar]

Beste ouder/verzorger,

Op onze school laten wij u met beeldmateriaal (foto's en video's) zien waar we mee bezig zijn. Opnames worden gemaakt tijdens verschillende gelegenheden. Bijvoorbeeld tijdens activiteiten, schoolreisjes en lessen. Ook uw zoon/dochter kan op dit beeldmateriaal te zien zijn.

Wij gaan zorgvuldig om met deze foto's en video's. Wij plaatsen geen beeldmateriaal waardoor leerlingen schade kunnen ondervinden. We plaatsen bij foto's en video's geen namen van leerlingen.
Daarnaast zijn wij vanuit de wetgeving verplicht om uw toestemming te vragen voor het gebruik van beeldmateriaal van uw zoon/dochter omdat hij/zij jonger is dan 16 jaar.

Het is goed om het geven van toestemming samen met uw zoon/dochter te bespreken. Als u uw keuze thuis bespreekt, dan weten ze zelf waarom het gebruik van foto's en video's wel of niet mag. Het is goed mogelijk dat u niet wilt dat foto's van uw kind op internet verschijnen.

Uw toestemming geldt alleen voor beeldmateriaal dat door ons of in onze opdracht wordt gemaakt. Het kan voorkomen dat andere ouders foto's maken tijdens schoolactiviteiten. De school heeft daar geen invloed op, maar wij vertrouwen erop dat deze ouders ook terughoudend zijn met het plaatsen en delen van beeldmateriaal op internet.

Met deze brief vragen we u aan te geven waarvoor [school] **beeldmateriaal van uw zoon/dochter mag gebruiken.**
Op het toestemmingsformulier kunt u zien voor welk doel de verschillende opties gebruikt worden.

Als we beeldmateriaal willen laten maken voor onderzoeksdoeleinden, bijvoorbeeld om een les van de stage- juf op te nemen, zullen we u daar apart over informeren en zo nodig om toestemming vragen. Ook als we beeldmateriaal voor een ander doel willen gebruiken, dan op het antwoordformulier vermeld staat, nemen we contact met u op.

U mag natuurlijk altijd de door u gegeven toestemming intrekken. Ook mag u op een later moment alsnog toestemming geven. Zonder toestemming zal er geen beeldmateriaal van uw zoon/dochter gebruikt en gedeeld worden.

Wilt uw het antwoordformulier met uw kind meegeven naar school?

Alvast bedankt voor uw medewerking!

Met vriendelijke groet,

[naam ondertekenaar]

Toestemmingsformulier gebruik beeldmateriaal (zie parnassys)
Toelichting gebruik formulier toestemming

Er is geen toestemming van ouders nodig voor het gebruik van beeldmateriaal in de klas en les voor onderwijskundige doeleinden. Ook is er geen toestemming nodig voor het plaatsen van een foto op een schoolpas of voor gebruik van een foto in het administratiesysteem. Wel gelden voor het gebruik van dat beeldmateriaal de gewone privacyregels (zoals dataminimalisatie: terughoudend omgaan met beeldmateriaal van leerlingen).

In het toestemmingsformulier is aparte toestemming opgenomen voor verschillende categorieën. De wetgever eist dat een ouder een goed geïnformeerde beslissing kan nemen, die ook **specifiek** is. Het vragen van toestemming 'voor gebruik van foto's door de school' is dat zeker niet. Als school mag je het dus niet zo formuleren: 'als u niet wilt dat we foto's van uw kind gebruiken, moet u dat maar zeggen'. Dit is een 'opt-out', en dit is in strijd met de wet.

Foto's maken door ouders op school
Het kan voorkomen dat ouders het vervelend vinden dat andere ouders foto's maken van hun kinderen.

Meestal overleggen deze ouders samen over het maken en gebruik van die foto's. Soms komen ouders er samen niet uit en dan wordt de school gevraagd om iets te regelen.

De school wil voor álle kinderen een veilige omgeving zijn, en niet een plek waar kinderen (en hun ouders) bang hoeven te zijn steeds te worden gefotografeerd. Het maken van foto's en video's op school kan moeilijk worden verboden, maar kan wel aan banden worden gelegd. Door bijvoorbeeld verwachtingen uit te spreken naar ouders over fotograferen tijdens een schoolactiviteit, of door ouders in de nieuwsbrief te vragen terughoudend te zijn met het maken en publiceren van foto's. Mocht dat niet het gewenste effect hebben, dan kan de schoolregels voor het maken van foto's op school vastleggen in het privacyreglement of in een aparte gedragscode of een protocol. Een schoolgebouw is niet zomaar een openbare plaats waar iedereen toegang toe heeft. De school kan aan het verlenen van toegang dus voorwaarden stellen zoals de (extreme) regel dat fotograferen van leerlingen tijdens de les of in klas alleen is toegestaan door docenten.

Als er beeldmateriaal op het beveiligde deel van de website door ouders gekopieerd wordt en vervolgens gedeeld via sociale media is dat niet meer de verantwoordelijkheid van de school. De school doet er wel goed aan om dit bij ouders onder de aandacht te brengen en hen te wijzen op hun verantwoordelijkheid hierin.

Toestemming geven door één of twee ouders
Het is de vraag of de toestemmingsverklaring door één of beide ouders moeten worden ondertekend.

Als leerlingen jonger zijn dan 16 beslissen de wettelijk vertegenwoordigers (de ouders) over de privacy. De wet gaat ervan uit dat je als school mag vertrouwen op de mededelingen van één ouder. Als dat vertrouwen terecht is, dan is de andere ouder ook gebonden aan die mededeling. Bij het ondertekenen van de toestemmingsverklaring, mag de school dus vertrouwen op de toestemming als één ouder die geeft. Alleen als de school weet dat de andere ouder (die niet getekend heeft) tegen de toestemming is, mag de school niet uitgaan van die ene ondertekening. Dan moet de school van beide ouders toestemming hebben. Vooral bij gescheiden ouders kan het verstandig zijn om de toestemming van beide ouders te vragen. Voor het intrekken van toestemming is de mededeling van één ouder ook voldoende.

Bij twijfel is het beter om te vertrouwen op twee handtekeningen, of om de foto dan maar niet te gebruiken.

Bijlage 16: Informatieplicht

Het realiseren van het IBP-beleid is voor een groot deel uit **informeren**. De AVG legt een wettelijke verplichting op met betrekking tot informatieverstrekking. De school informeert de betrokkene nog meer over hoe zij met hun persoonsgegevens omgaan.
De school is transparant over de privacyafspraken en -processen, en verstrekt proactief informatie erover. Dat betekent dat er op de website voldoende informatie is te vinden over hoe de school omgaat met persoonsgegevens, welke afspraken er zijn rondom privacy en welke maatregelen er zijn getroffen om de persoonsgegevens te beschermen.

Communiceren

De school praat met regelmaat over het belang van IBP en helpt om het bewustzijn bij iedereen te vergroten. Hieronder worden tips aangeboden hoe we met zowel medewerkers, leerlingen als ouders over deze onderwerpen een dialoog kunnen starten.

Dialoog met medewerkers

Beleid en maatregelen zijn niet voldoende om risico's op het gebied van IBP uit te sluiten. Meestal speelt de mens een belangrijke rol als er beveiligingsincidenten of datalekken zijn ontstaan. Daarom is het erg belangrijk om het bewustzijn bij de medewerkers te vergroten en aan te scherpen.

Bewustwording

Onderdeel van het IBP-beleid is dat er regelmatig terugkerende bewustwordingscampagnes voor medewerkers wordt georganiseerd. Aan alle medewerkers wordt regelmatig algemene scholing gegeven en specifieke trainingen georganiseerd voor groepen medewerkers die vaker met IBP te maken hebben.
Elke medewerker en ouder/leerling moet er van uit kunnen dat er altijd zorgvuldig met zijn of haar persoonsgegevens wordt omgegaan. Naleving van de wetgeving is wel de verantwoordelijkheid van de school, maar naleving en borging hiervan kan alleen bereikt worden wanneer iedereen binnen de schoolorganisatie zorgvuldig en verantwoord met persoonsgegevens weten om te gaan.

Om dit te faciliteren zijn er twee mogelijkheden:

1. De eerste is een model PowerPointpresentatie. Een medewerker, die belast is met IBP, geeft deze presentatie binnen zijn organisatie aan de medewerkers. Hij wordt hierbij ondersteunt door een inhoudelijke toelichting die in de notities van de slides zijn verwerkt: 'AVG presentatie' en Presentatie - IBP voor medewerkers.
2. Een tweede optie is dat medewerkers op eigen gelegenheid de online workshop "training bewustwording IBP voor medewerkers" in Wikiwijs kan doorlopen**: "training bewustwording IBP voor medewerkers"**

Dialoog met leerlingen

Ook leerlingen maken steeds meer gebruik maken van digitale middelen om te leren en te communiceren. Als je bedenkt dat 95% van de leerlingen in groep 8 een smartphone heeft en een groot deel actief is op sociale media, is het helemaal niet gek om in de klas het gesprek aan te gaan over hoe zij hun privacy kunnen bewaken. En hoe zij met de privacy van mede-leerlingen omgaan. Want mag je je wachtwoord met iemand delen? Maar ook; hoe gaan we met elkaar om op sociale media?
Naast slachtoffer op internet kunnen jongeren ook dader zijn. Door bijvoorbeeld de schoolwebsite te hacken of het systeem plat te leggen met een DDos(distributed) denial-of service)-aanval. Wanneer er anti-pestregels zijn, anti-pestcontract of een gedragscode ict- en internetgebruik, wordt dit meestal klassikaal besproken. Maar hoe praat je nu eigenlijk in de klas over informatiebeveiliging en privacy?

Hoe ga je het gesprek aan met leerlingen over IBP?

Hiervoor hebben we 25 hulpvragen opgenomen om met leerlingen van 10- tot 18-jaar het gesprek aan te gaan over deze twee moeilijke onderwerpen:

1. Het pdf bestand: 'dialoog met leerlingen 1': 25 Manieren om te vragen aan leerlingen: wat is voor jou het verschil tussen goed en fout op internet?

2. Het pdf bestand: ‘dialoog met leerlingen 2’: 25 manieren om te vragen aan leerlingen: hoe bewaak jij je privacy op internet?

Digitale geletterdheid
21e eeuwse vaardigheden worden gezien als competenties die leerlingen nodig hebben in een snel veranderende maatschappij waarin technologie een belangrijke rol speelt. Onderdeel van die vaardigheden is het onderwerp digitale geletterdheid dat bestaat uit de 4 vaardigheden
1. computational thinking,
2. mediawijsheid,
3. informatievaardigheden en
4. ict-basisvaardigheden.

Deze laatste vaardigheid gaat over het kennen van basisbegrippen en functies van computers en netwerken, het kunnen aansluiten en bedienen van hardware. Maar ook het kunnen omgaan met kantoortoepassingen, zoals tekstverwerkers en presentatiesoftware. En kunnen werken met internet, met mobiele apparaten en op de hoogte zijn van beveiligings- en privacyaspecten.

Sociale media; maak iedereen mediawijs
Digitale geletterdheid speelt ook in op beveiligings- en privacy aspecten.
Mediawijsheid omvat hier de kennis, vaardigheden en mentaliteit die nodig zijn om bewust, kritisch en actief om te gaan met media. Deze zijn onderverdeeld in:

- **Begrip**: inzicht hebben in de medialisering van de samenleving, begrijpen hoe media gemaakt worden, zien hoe media de werkelijkheid kleuren.
- **Gebruik**: apparaten, software en toepassingen gebruiken, je kunnen oriënteren binnen mediaomgevingen.
- **Communicatie**: informatie vinden en verwerken, content creëren, participeren in sociale netwerken.
- **Strategie**: reflecteren op het eigen mediagebruik, doelen realiseren met media.

Veilig online

De school gebuikt deze **filmpjes** van Alert Online om leerlingen te laten zien wat ze moeten doen om veilig online te zijn.

(D)Dos; Van kattenkwaad tot strafblad
Naast slachtoffer op internet kunnen jongeren ook dader zijn. Een (D)Dos (distributed) denial-of service)--aanval op school, dat kan iedereen overkomen… Het uitvoeren van een (D)Dos-aanval is strafbaar volgens de wet, met een maximale celstraf van 6 jaar. Bewustwording van de gevolgen van het uitvoeren van een (D)Dos-aanval en het hebben van een strafblad is belangrijk voor betrokkene. Zie voor meer informatie over (D)DoS de rubriek (D)DoS, wat moet ik weten.

Dialoog met ouders
Scholen verzamelen en gebruiken steeds meer persoonsgegevens van en over leerlingen. De school is wettelijk verplicht om te verantwoorden wat zij met die gegevens doet. Ouders, en leerlingen (als zij 16 jaar en ouder zijn), hebben het recht om (ongevraagd) in begrijpelijke taal, uitgelegd te krijgen hoe privacy op jouw school is geregeld.
Als de school vragen over privacy heeft dan moet de school deze kunnen beantwoorden en hen uit kunnen leggen wat de school doet met de gegevens van hun kinderen. We beschrijven hier een aantal onderwerpen waar ouders regelmatig vragen over hebben.

Privacy bijsluiter
Om uit te leggen welke afspraken de school heeft gemaakt met uitgevers, distributeurs of leveranciers van software, verwijst zij naar de privacy bijsluiter die bij de bewerkersovereenkomsten zit. In de privacy bijsluiter vertelt de leverancier wat het product doet, welke gegevens hij gebruikt en wat het doel van dat gebruik is.

Wees transparant over privacy

Als ouders het vertrouwen hebben dat de school IBP goed heeft geregeld, dan zullen ze veel sneller bereid zijn om gegevens te delen.

Filmen en fotograferen door ouders
De school maakt afspraken over het gebruik van foto's van leerlingen voor de website, schoolgids enz. Ouders moeten hiervoor specifiek toestemming geven en bezwaar kunnen maken als zij niet willen dat een foto van hun kind hiervoor gebruikt wordt.
Maar wat doe je met ouders die op school foto's maken? Hoe ga je om als ouders foto's van de beveiligde site kopiëren en vervolgens delen? Het is aan de school hoe zij hiermee omgaan. Verbieden is lastig, maar afspraken maken kan een oplossing zijn. (Zie pdfbestand: 'Filmen en fotograferen door ouders'.)

Wat is de rol van de (G)MR rondom privacy?
Het is verstandig om ook jaarlijks met de (G)MR te praten over hoe de school omgaat met leerlinggegevens. Openheid en transparantie over het gebruik van leerlinggegevens is het uitgangspunt in alle communicatie met ouders! De MR heeft ook instemmingsrecht als het gaat over onderwerpen waarbij privacy van leerlingen en medewerkers een rol spelen. Zo moet het privacyreglement worden goedgekeurd door de (P)MR.

Mogen grootouders en pleegouders ook vragen om inzage?
Bij leerlingen onder de 16 jaar heeft de wettelijk vertegenwoordiger het gezag over het kind en beslist namens het kind over de privacy. Dat zullen in de meeste gevallen één of beide ouders zijn. Maar ook pleegouders, die officieel het gezag over het kind hebben, hebben recht op inzage van het dossier. Grootouders mogen het dossier van hun kleinkind niet inzien dat ligt anders, zij zullen niet snel de wettelijk vertegenwoordiger zijn.

Bijlage 17: Risicoanalyse waarom?

Risico Analyse: school in kaart

1. De situatie op school: hoe ziet de school eruit?

Doelgroepen

1. Personeel
2. Leerlingen
3. Ouders
4. Gasten (stagiares, aanbieders, externen)

Bewerking gegevens doelgroepen

1. Gegegevens in de cloud
    a. Website school
        i. Geen risico gegevens
    b. Vensters.nl
        i. Geen risico gegevens
    c. Social media
        i. Foto's gemaakt op school (gezicht afgeschermd, maar niet altijd)
        ii. Video's opnames gemaakt op school
    d. Raet
        i. Login digitale omgeving personeel financiele gegevens
    e. Verzuimsignaal
        i. NAW gegevens personeel
        ii. Ziekte status personeel
        iii. Gespreksverslagen arbo arts zieke personeel
        iv. Verzuimdossier
        v. In afwachting reactie
    f. Schoolserver
        i. Netwerkschijven
            1. Gegevens leerlingen
                a. Ontwikkelingperspectief
                b. Leerlingdossiers
                c. Rapporten
                d. Gesprekken ouders
                e. Foto's
                f. Video's
        ii. Printserver koppeling
    g. Werkplekken personeel
            1. Papierwerk gegevens leerlingen of ouders op bureau
    h. Office 365
            . One drive
            i. Email
            ii. Etc.
    i. ParnasSys
            . Leerlingadministratie
        1. Naw gegevens
        2. Leerlingendossiers
        3. Leerresultaten
        4. Medische gegevens
    j. Groenendijk administratie
            . NAW gegevens
            i. BSN nummer
            ii. Salarisstroken
            iii. In afwachting reactie

k. Software uitgevers (malmberg, zwijssen, noordhoff uitgevers, momento, basispoort)
    . In afwachting reactie uitegeverij
l. Cito LOVS
    . In afwachting reactie
m. Oefenweb
    . Schooljaar
    i. Brincode
    ii. Groep
    iii. Volledige Naam
    iv. Namen leerkrachten
    v. Geslacht
n. Nieuwsbegrip
    . Schooljaar
    i. Brincode
    ii. Groep
    iii. Volledige Naam
    iv. Namen leerkrachten
    v. Geslacht
o. ELK amsterdam
    . In afwachting reactie
p. Voip telefonie
    . In afwachting reactie
q. QLICT | de Rolfgroep
r. Forehand | Aerohive wifi
    . Gebruik toestel
    i. Naam toestel
    ii. Type browser
    iii. Wachtwoorden SSID's
s. Chromebooks | G-suite omgeving
    . Emails en wachtwoorden leerlingen
t. 2ICT | Cloudtrax
    . Gebruik toestel
    i. Naam toestel
    ii. Type browser
    iii. Wachtwoorden SSID's
u. Kyocera
    . In afwachting reactie
v. BOA glasvezel leverancier
    . In afwachting reactie
w. Printer
    . Opslag harde schijf van taken

2. Gegevens buiten de cloud om
a. Laptops personeel (wordt lokaal op gewerkt)
    . Niet bekend wat er opgeslagen word
b. Opslag gegevens leerlingen en personeel op papier | archief
c. Beeld en geluidopnames intern gebruik

Risicoanalyse in beeld

Powerpoint presentatie: AVG Presentatie

Voorlichtingslessen leerlingen groep 7 en 8

Privacy gaat iedereen aan, ook onze leerlingen. Wij dienen onze leerlingen bewust te maken van wat privacy is. De autoriteit persoonsgegevens heeft daarom een informatief lessenpakket samengesteld. Zie link: https://primaindeklas.nl/lesson/index/314?hash=46c9614f

Bijlage 18: Gedragscode gebruik informatievoorziening

De gedragscode is een regeling die de gedragsregels beschrijft voor individuele gebruikers van Informatievoorzieningen van de school. Deze regeling maakt onderdeel uit van het informatiebeveiligingsbeleid en is van toepassing op iedereen die gebruik maakt van Informatievoorzieningen aangeboden door de school. In de gedragscode staan gedragsregels hoe met het gebruik van informatievoorziening moet worden omgegaan. Mocht de naleving ernstig tekortschieten, dan kan de school de betrokken verantwoordelijke medewerkers een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

De afspraken zijn verdeeld in drie onderdelen:

1. Hoe zorg ik dat ik op een veilige manier om ga met vertrouwelijke gegevens?

2. Hoe ga ik veilig om met leerlinggegevens?

3. Internet en sociale media

Hieronder volgen per onderdeel de afspraken.

A. Hoe zorg ik dat ik op een veilige manier om ga met vertrouwelijke gegevens?

1. Zorg ervoor dat je papieren met daarop vertrouwelijke gegevens altijd achter slot en grendel liggen.

2. Indien je papieren met daarop vertrouwelijke gegevens wilt vernietigen doe je dit altijd door een papierversnipperaar. Ook als je thuis werkt.

3. Zorg erbij vertrouwelijke (telefonische) gesprekken voor dat er niet kan worden meegeluisterd. Trek je je even terug als een gesprek een vertrouwelijk karakter heeft of krijgt.

4. Thuis wordt er alleen in de cloud (Office 365) gewerkt en worden er geen documenten en of foto’s van leerlingen opgeslagen.

5. Bewaar laptops of tablets altijd op een veilige plek, zeker tijdens vakantieperiodes.

6. Maak elkaar er dus op attent als je een laptop of tablet onbeheerd ziet liggen. Als je computer gestolen wordt, heeft dat gevolgen voor de school en de leerling. Als je privé laptop gestolen wordt waarop toch onverhoopt documenten en of foto’s van school staan meldt dit altijd direct bij de leidinggevende.

7. Klik alleen op linkjes en open alleen bijlagen in e-mails van betrouwbare afzenders en pas op met het downloaden van bestanden. Virussen kunnen makkelijk worden binnengehaald via (phising)mails. In het criminele circuit is dit een veelgebruikte methode om aan jouw gegevens te komen. Ook kunnen de gegevens op je computer versleuteld worden (ransomeware). Mocht dit ongewild toch gebeuren meldt dit direct bij de leidinggevende.

8. Houd je eigen aan het wachtwoordbeleid

9. Meld je altijd af als je de computer onbeheerd achterlaat. Maak er een gewoonte van om papieren op je bureau om te draaien. Zo voorkom je dat anderen informatie zien die niet voor hen is bedoeld.

10. Zet je digibord op freeze als je wachtwoorden intoetst of persoonsgegevens in je scherm ziet staan. En zorg dat niemand meekijkt als jij je wachtwoord intoetst. Voordat je het weet zien leerlingen gevoelige gegevens of kunnen ze aan de hand van je afgekeken gebruikersnaam en wachtwoord proberen in te loggen.

11. Zet de notificatie-functie van je e-mail uit, zodat er tijdens je les geen meldingen op het bord binnen komen die leerlingen kunnen zien, maar niet voor hun ogen bestemd zijn.

12. Zorg dat men van buitenaf niet kan meelezen op jouw beeldscherm.

13. Zorg voor een clear desk als je van je werkplek weggaat.

B. Hoe ga ik veilig om met leerlinggegevens

1. Verwerk leerlinggegevens zoveel mogelijk digitaal.

2. Leerlinggegevens worden zoveel mogelijk digitaal opgeslagen, geraadpleegd en bewerkt. Dit geldt ook voor gegevens die via ouders/verzorgers en/of externen worden ontvangen. Bewaar geen gegevens op een USB-stick. Gegevens die op papier aangeleverd worden, worden gescand en in de Cloud bewaard. Vergeet niet om de scan van je eigen computer te verwijderen.

3. (Persoons)Gegevens die niet in het administratiesysteem horen, bijvoorbeeld foto's, worden altijd in de juiste map opgeslagen in server van de school.

4. Formuleer gegevens die je vastlegt over een persoon zorgvuldig en professioneel. Ouders hebben het recht om het dossier in te zien. Zorg ervoor dat de gegevens zodanig zijn geformuleerd dat dit kan. Het past ook bij je houding als onderwijsprofessional.

5. Gebruik voor de verwerking van leerlinggegevens bij voorkeur een computer van de school. Moet je leerlinggegevens downloaden en bewerken op je privé computer? Doe dit alleen op een beveiligde computer (die voorzien is van encryptie), bij voorkeur een computer van school. Verwijder de bestanden na gebruik van je computer. Zorg ervoor dat anderen (bijv. familieleden) niet bij jouw werkbestanden kunnen komen.

6. Thuis printen? Zorg ook hier dat je de gegevens achter slot en grendel opslaat en z.s.m. mee naar school neemt en het daar opbergt in de juiste map. Indien je de papieren vernietigt doe je dit altijd via een papiervernietiger.

7. Ga na welke afspraken er binnen de school gemaakt zijn voordat je gegevens uitwisselt met derden.

8. Wanneer je gegevens uit wil wisselen met externen, zoals bijvoorbeeld de logopedist, een arts, jeugdzorg of een schoolbegeleidingsdienst dan is het nodig om toestemming te vragen van ouders. Zorg dat je de toestemming registreert en hou daarbij ook rekening met de verdeling van het ouderlijk gezag. Voor de uitwisseling van gegevens met het samenwerkingsverband of een andere school gelden aparte afspraken. Hiervoor kun je terecht bij FG.

9. Informeer derden (ouders, hupverleners etc.) wanneer je door hen aangeleverde informatie (zowel geschreven als mondeling) opslaat in het leerling dossier.

10. Wanneer je bijvoorbeeld telefonisch contact hebt over een leerling met een hulpverlener en je wilt die informatie opslaan in het leerling dossier. Informeer dan zowel de hulpverlener als de ouders welke informatie je aan het dossier toevoegt.

C. Internet en sociale media

Hoe en wat communiceer ik online?

1. Als je leerlinggegevens per mail stuur het dan versleuteld. Anders verstuur je een link met de vindplaats van de benodigde gegevens in Onedrive of Google Drive.

2. Vraag ouders om toestemming om een (privé)account aan te maken voor online diensten indien je deze wilt gebruiken in je lessen. Leerlingen moeten toestemming hebben van hun ouders/verzorgers om een (privé)account aan te maken voor online diensten zoals Prezi, Pinterest, Canva etc.

3. Geef nooit persoonsinformatie via een binnengekomen telefoontje, bel altijd terug zodat je zeker weet dat je spreekt met de persoon die de informatie mag vragen. Bij twijfel altijd overleggen met de leidinggevende.

4. Hou je aan het internet en sociale media protocol

5. Het is voor medewerkers van de school niet toegestaan standpunten en/of overtuigingen uit te dragen die strijd zijn met de missie en visie van de school.

6. Ga voordat je foto's of video's publiceert waar leerlingen op te zien zijn na of ouders hiervoor toestemming hebben gegeven.

7. Publiceer geen foto's van leerlingen op je eigen Sociale Media. De ouders geven toestemming aan de school niet aan jou.

8. Externe begeleiders in (scholings) trajecten die gebruik willen maken van video en of foto opnames gemaakt tijdens dit traject moeten hiervoor toestemming vragen aan de ouders van de leerlingen die hierin zichtbaar zijn, alsmede aan de leerkrachten.

9. Gebruik de accounts die door de school worden beheerd als je met ouders of leerlingen wil communiceren via e-mail of sociale media. Gebruik nooit privé accounts voor communicatie met ouders.

10. Formuleer je boodschap ook hier professioneel en zorgvuldig, in correcte taal.

11. Zet e-mailadressen altijd in de BCC-regel als je naar meerdere mensen een bericht verstuurt. Zo blijven de e-mailadressen van iedereen afgeschermd. Gebruik ook bcc als je al je collega's mailt, zo voorkom je dat men bij beantwoorden (per ongeluk) op de knop alle beantwoorden klikt.

12. Stuur nooit een e-mailbericht door naar derden zonder de degene van wie je het bericht ontvangen hebt hierover te informeren.

13. Wanneer je een bericht stuurt met belangrijke en/of gevoelige informatie naar (een groep) ouders/verzorgers laat dit dan nalezen door een collega. Een foutje is snel gemaakt en bovendien kan een ander je boodschap anders interpreteren dan jij hem bedoeld hebt. Het is dan fijn als er iemand met je meeleest voordat je hem verstuurt.

Bijlage 19: Protocol social media

Inleiding

Social media zijn een verzamelbegrip voor online platformen waar de gebruikers, zonder of met minimale tussenkomst van een professionele redactie, de inhoud verzorgen. Onder de noemer social media worden onder andere weblogs of blogs, social bookmarking, videosites als YouTube, Vimeo, fora, op samenwerking gebaseerde projecten als Wikipedia, en sociale netwerken als Facebook en Google+ geschaard. Via deze media delen mensen verhalen, kennis en ervaringen. Dit doen zij door berichten te publiceren of door gebruik te maken van ingebouwde reactiemogelijkheden. Voorbeelden van dit laatste zijn weblogs, waar lezersreacties achterlaten door middel van een reactieformulier of trackbacks.

Er is discussie over de vraag of WhatsApp deel uitmaakt van het begrip social media. Omdat blijkt dat ook met ouders gebruikt gemaakt wordt van app groepen, is in dit protocol aandacht gegeven aan WhatsApp.

Social media bieden de mogelijkheid om te laten zien dat je trots bent op de school en kunnen een bijdrage leveren aan een positief imago bij ouders, deelnemers, leveranciers en vakcollega's etc. Het delen van informatie en kennis met groepen waarmee op traditionele wijze nauwelijks communicatie mogelijk was kan leiden tot een beter beeld van de organisatieomgeving. Van belang is te beseffen dat je met berichten op social media (onbewust) de goede naam van de school en betrokkenen ook kunt schaden. Om deze reden vragen wij om bewust met de social media om te gaan.

Essentieel is dat de gebruikers van social media tegenover alle betrokkenen de reguliere fatsoensnormen in acht blijven nemen en de nieuwe mogelijkheden met een positieve instelling benaderen.

De school vertrouwt erop dat haar medewerkers en andere betrokkenen verantwoord om zullen gaan met social media en heeft dit protocol opgezet om een ieder die bij de school betrokken is of zich daarbij betrokken voelt daarvoor richtlijnen te geven.

Uitgangspunten:

1. De school onderkent het belang van social media.

2. Dit protocol draagt bij aan een goed en veilig werkklimaat;

3. Dit protocol bevordert dat de organisatie en zijn medewerkers op de social media communiceren in het verlengde van de missie en visie van de school en daarbij de reguliere fatsoensnormen in acht nemen. In de regel betekent dit dat we respect voor de organisatie en elkaar hebben, dat we verdraagzaam zijn en iedereen in zijn waarde laten;

4. De gebruikers van social media dienen rekening te houden met de goede naam van de school en van een eder die betrokken is bij de school;

5. Het protocol dient ervoor om alle betrokkenen bij de organisatie te beschermen tegen de mogelijke negatieve gevolgen van de social media;

Doelgroep en reikwijdte:

1. Deze richtlijnen zijn bedoeld voor alle betrokkenen die deel uitmaken van de school, dat wil zeggen medewerkers, stagiaires en mensen die op een andere manier verbonden zijn aan de school.

2. De richtlijnen in dit protocol hebben alleen betrekking op berichten die gerelateerd zijn aan de school of wanneer er sprake is een overlap is tussen werk en privé.

Social media, de Algemene Verordening Gegevensbescherming (AVG) en de organisatie:

A. Voor alle medewerkers

1. Het is betrokkenen toegestaan om kennis en informatie over de organisatie en de leden van de school te delen, mits die informatie niet vertrouwelijk is en het geen persoonsgegevens betreft en andere betrokkenen niet schaadt.

2. Medewerkers zijn persoonlijk verantwoordelijk voor de inhoud die ze, voor zover dat niet tot hun functie behoort, publiceren op blogs, wiki's, fora en andere media die gebaseerd zijn op user-generated content.

3. Elke betrokkene dient zich ervan bewust te zijn dat de gepubliceerde teksten en uitlatingen voor onbepaalde tijd openbaar zullen zijn, ook na verwijdering van het bericht.

4. Wees extra voorzichtig bij het publiceren over, of in discussie gaan met, een ouder of organisatie. Verkeerd opgevatte of slecht onderbouwde stukken, kunnen direct nadelige gevolgen hebben voor de school.

5. De school vraagt aantoonbaar schriftelijke toestemming aan medewerkers om foto-, film- en geluidsopnamen van aan organisatie gerelateerde situaties, waarop zij zijn afgebeeld, op de zakelijke en/of persoonlijke social media te zetten.

6. Alle betrokkenen nemen de reguliere fatsoensnormen tegenover betrokkenen binnen de organisatie in acht. Als fatsoensnormen worden overschreden (bijvoorbeeld: hacken van een account, pesten, kwetsen, stalken, bedreigen, radicalisering, zwartmaken of anderszins beschadigen) dan neemt de school passende maatregelen.

7. Een medewerker kan een professionele groepsapp maken ten behoeve van een klas welke hij/zij begeleid. Dit ten behoeve van het door hem doorgeven van bijzondere aangelegenheden zoals bijvoorbeeld uitval, het opgeven van huiswerk, het herinneren aan bijeenkomsten. De instellingen moeten dan wel zo zijn, dat de medewerker de enige is die berichten kan versturen. Leden van de groep kunnen alleen middels privé berichten antwoorden. Zie uitleg * onderaan dit document.

8. Medewerkers hebben een bijzondere verantwoordelijkheid bij het gebruik van social media: privémeningen van medewerkers kunnen eenvoudig verward worden met de officiële standpunten van de school.

9. Indien een medewerker deelneemt aan een discussie die (op enigerlei wijze) te maken heeft met de school dient de medewerker te vermelden dat hij medewerker is van de school en welke functie hij heeft.

10. Als onlinecommunicatie dreigt te ontsporen dient de medewerker direct contact op te nemen met zijn leidinggevende om de te volgen strategie te bespreken.

11. Bij twijfel of een publicatie in strijd is met deze richtlijnen neemt de medewerker contact op met zijn leidinggevende.

B. Voor medewerkers tijdens privésituaties

1. Het is de medewerker toegestaan om werk gerelateerde onderwerpen te publiceren mits het geen persoonsgegevens de school, haar medewerkers of andere betrokkenen betreft. Ook mag de publicatie de naam van de school niet schaden.

2. Het is voor medewerkers niet toegestaan standpunten en/of overtuigingen uit te dragen die in strijd zijn met de missie en visie van de school en de uitgangspunten van dit protocol.

3. Indien een medewerker deelneemt aan een discussie die (op enigerlei wijze) te maken heeft met de school dient de medewerker te vermelden dat hij medewerker is van de school en welke functie hij heeft.

4. Als de medewerker over de school publiceert dient hij het bericht te voorzien de mededeling dat de standpunten en meningen in dit bericht de eigen persoonlijke mening zijn (op persoonlijke titel zijn geschreven) en los staan van eventuele officiële standpunten van de school.

Sancties en gevolgen voor medewerkers

1. Medewerkers die in strijd handelen met dit protocol maken zich mogelijk schuldig aan plichtsverzuim. Alle correspondentie over dit onderwerp wordt opgenomen in het personeelsdossier.

2. Indien de school de wijze van communiceren door een medewerker(s) als 'grensoverschrijdend' kwalificeert, dan wordt dit telefonisch gemeld bij de Landelijke Vertrouwensinspecteur (0900 – 1113111).

3. Afhankelijk van de ernst van de uitlatingen, gedragingen en gevolgen worden naar medewerkers toe rechtspositionele maatregelen genomen die variëren van waarschuwing, schorsing, berisping, ontslag en ontslag op staande voet;

** WhatsApp*

WhatsApp heeft een nieuwe functie in chatgroepen. Als een beheerder van een groepschat de functie inschakelt, kan hij als enige berichten naar de groep versturen. De leden kunnen de berichten alleen lezen, en desgewenst een privé-bericht naar de beheerder sturen. De groep blijft zo een overzichtelijk kanaal met updates. Om deze functie uit te voeren open je WhatsApp en tap je op de naam van de groep helemaal bovenaan. Vervolgens kies je voor "Groepsinstellingen" en bij het volgende scherm kies je "Alleen beheerders" bij "Berichten versturen".