Uitgangspunten

Op deze pagina worden achtereenvogens de volgende punten besproken:
(klik op de titel om meer informatie te verkrijgen.)

Informatiebeveiliging en privacy (IBP)

Met informatiebeveiliging beschermen we onze school tegen risico's en bedreigingen met betrekking tot informatie en ict. Het richt zicht op drie aspecten:

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

Privacy gaat om de bescherming van persoonsgegevens conform de huidige wet- en regelgeving. Door het goed toepassen van informatiebeveiliging kan aan deze wetgeving worden voldaan.

Beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten zijn:

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

Vijf vuistregels voor Privacy

We hanteren de volgende vijf vuistregels:

- **Doelbepaling en doelbinding:**
  Persoonsgegevens worden alleen gebruikt waar dit nodig is voor het functioneren van de school. Deze doeleinden zijn in de documentatie rondom privacy op SVOSW in detail beschreven.
- **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.
- **Dataminimalisatie:**
  Bij de verwerking van Persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: er worden niet meer gegevens opgeslagen en verwerkt dan dat strikt noodzakelijk is om het doel te bereiken. Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk en wettelijk is vastgelegd.
- **Transparantie:**
  De school legt aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens en het hierop gevoerde beleid. Daarnaast hebben deze betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens (audit).
- **Data-integriteit:**
  Er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

Verantwoordelijkheden

Naast de algemene verantwoordelijkheid voor de informatiebeveiliging en privacy die geldt voor alle medewerkers van de stichting, dragen ondestaande functionarissen een speciale verantwoordelijkheid voor de privacy:

- **Eindverantwoordelijke**:
  Het College van Bestuur is eindverantwoordelijk voor de informatiebeveiliging en privacy.
- **Functionaris voor Gegevensbescherming:**
  De functionaris voor gegevensbescherming (FG) houdt binnen SVOSW toezicht op de toepassing en naleving van de privacy-wetgeving. De FG is ook contactpersoon en voor klachten en vragen van betrokkenen met een vertrouwelijk karakter.
- **Privacy Officer**:
  De privacy officer (PO) vormt een aanspreekpunt voor de uitvoering van de 'informatiebeveiliging en privacy' en de afhandeling van incidenten inclusief auditaanvragen.

N.b. deze taken zijn nog in ontwikkeling. Het kan zijn dat hier nog het e.e.a. aan verandert.

Incidenten en datalekken

Alle incidenten kunnen worden gemeld bij de Privacy Officer van de school. De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken.

Afbeelding: Vijf vuistregels voor privacy