Privacykaart INNOVO-medewerkers

Begrippen

IBP: Informatiebeveiliging en privacy; betreft het beveiligen van privacygevoelige gegevens en het correct omgaan met de privacy van personen.

AVG: Algemene verordening gegevensbescherming is de wettelijke basis van de IBP.

Privacy: Privacy is een grondrecht en omvat het recht om met rust te worden gelaten; het recht om te weten en te bepalen wat er met gegevens over jou gebeurt en om te weten wie de beschikking heeft over jouw gegevens.

Persoonsgegevens: Privacywetgeving gaat over persoonsgegevens en dat zijn alle gegevens, waarmee direct of indirect een natuurlijk persoon (mens) kan worden geïdentificeerd. Denk aan: naam, BSN-nummer, geboortedatum, telefoonnummer of IP-adres; maar ook aan het volgen of vastleggen van gedrag, handelen van personen via foto's, films, schoolwebsite, *social media*, e.d.

Bijzondere persoonsgegevens: Gevoelige informatie over leerlingen en medewerkers, zoals informatie over gezondheid, gedragsproblemen, politieke voorkeur, godsdienst, seksuele voorkeur of een problematische thuissituatie. Deze mogen niet worden gebruikt, tenzij de wet daar toestemming voor geeft.

Privacygevoelige gegevens: Persoonsgegevens en Bijzondere persoonsgegevens.

Verwerken: Alles wat er met persoonsgegevens wordt gedaan, valt onder de wettelijke bescherming: *on-line* en *off-line* persoonsgegevens verzamelen, kopiëren, opslaan, verspreiden, publiceren, delen én uitwisselen.

Toestemming van een betrokkene: Een bewuste, actieve handeling van de betrokkene, waaruit blijkt dat deze uitdrukkelijk akkoord gaat dat zijn/haar persoonsgegevens, of van zijn/haar kinderen tot 16 jaar, worden verwerkt. Het moet duidelijk zijn waar specifiek toestemming voor wordt gevraagd: vooraf is de betrokkene geïnformeerd voor welk doel de gegevens gebruikt gaan worden. Een *opt-out* – geen bezwaar, tenzij gemeld - is geen goedkeuring, evenmin als een toevoeging op een aanmeldformulier of via aanpassing van de schoolregels. Ouders moeten periodiek ondubbelzinnig toestemming hebben gegeven door plaatsing van een handtekening. Ouders worden tenminste één keer per jaar specifiek gevraagd een keuze te maken voor de handhaving van de toestemming of intrekking daarvan. INNOVO hanteert daartoe centraal een *toestemmingformulier* dat via de ouderportal wordt ingevuld.

Beveiligingsincident: Van een beveiligingsincident is sprake, wanneer er iets gebeurt met informatie en/of informatiesystemen, waarbij de kans aanwezig is dat de vertrouwelijkheid, de integriteit of de beschikbaarheid hiervan in gevaar is, of kan komen.

Datalek: Een datalek is een beveiligingsincident, waarbij het risico groot is dat onbevoegden zich toegang kunnen verschaffen tot persoonsgegevens. Er is dan sprake van verloren raken van persoonsgegevens of van een onrechtmatige verwerking, wanneer mogelijke toegang tot persoonsgegevens door onbevoegden redelijkerwijs niet kan worden uitgesloten. Voorbeelden van een datalek zijn het verlies van een USB-stick of laptop met privacy-gevoelige gegevens, of het sturen van een mailing met adressen in het CC-veld (in plaats van het BCC-veld), verlies van inlog-gegevens, school- of werkprestaties.

Een datalek moet binnen 72 uur via INNOVO gemeld worden bij de toezichthouder.

Vijf Vuistregels:

1. **Doel en doelbinding :** Worden persoonsgegevens uitsluitend gebruikt voor dat doel dat ik vooraf heb vastgelegd?
2. **Grondslag:** Kan ik aantonen, dat ik deze gegevens mag verwerken? Is er minimaal één wettelijke grondslag voor de verwerking? Heb ik toestemming of is er een gerechtvaardigd belang.
3. **Dataminimalisatie:** Gebruik ik alleen die minimale gegevens, die noodzakelijk zijn om het vastgestelde doel te verwezenlijken? Kan ik met minder of bijvoorbeeld met anonieme gegevens werken? Bewaar ik de gegevens niet langer dan strikt nodig?
4. **Transparantie:** Heb ik de leerling en/of de ouders vooraf uitgelegd, waarom welke gegevens worden gebruikt en met wie deze worden gedeeld?
5. **Data-integriteit:** Kloppen de persoonsgegevens die ik gebruik nog steeds? Zijn de gegevens voor de juiste mensen beschikbaar? Heb ik onjuiste gegevens gecorrigeerd of verwijderd?

Do's en don'ts

1. **Wachtwoorden**: Ga zeer zorgvuldig om met wachtwoorden; niet makkelijk te raden, nergens noteren, niet uitlenen en niet vaker hetzelfde wachtwoord gebruiken: een mix van minimaal 8 tekens.
2. **E-mailen:** Er mogen geen privacygevoelige gegevens per mail worden verstuurd. Niet in de tekst en niet in de bijlagen. Per post is ook onvoldoende veilig, tenzij aangetekend. Wel is het mogelijk om het bestand te '*zippen*' of in PDF te zetten en te voorzien van een wachtwoord. Geef het wel het beveiligingswachtwoord op een andere manier door aan de ontvanger.
3. **E-mail adressen:** Het gebruik van verzendgroepen moet altijd via het BCC-adresveld gebeuren. Het gebruik van de pop-up met recent gebruikte e-mailadressen is een risico. Dubbel controleren.
4. **Beeldmateriaal:** Foto's en video's van leerlingen zijn persoonsgegevens. Een openbaar toegankelijk fotoalbum, maar ook publiceren op Facebook of andere *social media*, is niet toegestaan. Alleen foto's van kinderen, waarvan de ouders toestemming hebben gegeven, mogen intern binnen school worden gedeeld. Het maken van foto's in je eigen groep als vorm van eigen aantekeningen mag wel, voor zover ze verder niet worden gedeeld of in het leerlingendossier worden opgeslagen.
5. **USB-sticks, HD:** Privacygevoelige gegevens mogen niet worden opgeslagen op USB-stick, memory-kaartjes, externe HD of andere mediadragers. Dit geldt ook voor privé-laptops, tablets of PC's en voor *devices* op school, die niet door de netwerkbeheerder worden beheerd. Privacygevoelige data mag alleen in de afgeschermde datamappen worden opgeslagen of in de digitale volgsystemen zoals Eduscope, Cito, Kijk, etc. De *Mijn Documenten*-map of andere persoonlijke mappen zijn niet toegestaan voor opslag van privacygevoelige gegevens, behalve voor 'eigen aantekeningen'.
6. **Printen:** Alle printopdrachten gaan standaard naar de mailbox van de printer, die vervolgens via een persoonlijke code benaderbaar is.
7. **PC Vergrendelen:** Voordat je het lokaal/de werkplek verlaat, moet de PC vergrendeld worden. Gebruik Windows-toets – L.
8. **Papieren dossiers:** Privacygevoelige documenten worden voortaan gescand en digitaal opgeslagen. Bestaande papieren dossiers of eigen aantekeningen liggen steeds achter slot en grendel ook bij korte afwezigheid.
9. **Gegevens verstrekken:** Geef niet zomaar informatie over een leerling door aan externen en dat geldt ook voor ouders/verzorgers die geen gezag hebben. Vragen? Raadpleeg het document "Gegevensverstrekking".

Thuiswerken

10. **Wachtwoorden:** Opslaan in je Google of Microsoft-account is niet toegestaan. Alleen op school/SEB mag gekozen worden voor wachtwoorden opslaan onder Windows. Schoon de opgeslagen wachtwoorden in Google of Microsoft op via wachtwoordenbeheer.
11. **Wachtwoorden:** Opslaan in een digitale wachtwoordkluis mag wel. Aanbevolen is *lastpass* (free) die zowel thuis als op het werk (online) kan worden ingezet. (www.lastpass.com)
12. **Inloggegevens:** Inloggegevens, die toegang geven tot telewerken of andere programma's met privacy-gevoelige gegevens, mogen thuis niet worden opgeslagen door Windows, Google of Microsoft.
13. **Webbased programma's**: Werken in webbased programma's zoals Eduscope, LDOS, Afas Insite, IGROW en Clooser mag ook thuis. Bestanden openen en downloaden in deze programma's mag alleen via telewerken of op school, omdat gedownloade bestanden lokaal in een downloadmap worden opgeslagen.