BELEIDSSTUK AVG Privacy Notitie

Naam: privacy notitie

Vastgesteld door bestuur op
Geïmplementeerd op 20-2-2020
Update: 13-05-2024

PRIVACY Notitie - kernpunten die iedere HSN-er weet en toepast

Voor privacy en veiligheid wordt door ouders en overheid aandacht gevraagd. Dat is terecht; de kinderen, en hun gegevens, worden ons toevertrouwd. Iedereen in de HSN werkt vanuit de 3 V's van Vakmanschap, Verantwoordelijkheid en Vertrouwen.
Er staat op de website een Privacyreglement - en meer - dat voor alle HSN-scholen geldt. Daarvoor is wel nodig dat bij alle medewerkers de inhoud bekend is. Datalekken ontstaan bijna nooit door mensen van buitenaf. Het is vastgesteld dat de meeste datalekken door eigen mensen worden veroorzaakt. Meestal gaat het om een fout geadresseerde email.
Daarnaast ontstaan beveiligingsincidenten het meest door een klik op een foute link. De gevolgen kunnen enorm zijn voor de hele organisatie. DAAROM:

- Alle (ook eigen) apparaten – vaak laptops - die je gebruikt in/voor je werkomgeving heb je beveiligd met een wachtwoord/code. Een telefoon, leerkracht-iPad, laptop geef je een toegangscode
- Wachtwoorden houd je voor jezelf. Heb je toch een keer een wachtwoord gedeeld, genoemd, of met het digibord aan in een verkeerd veld ingevuld, dan pas je je wachtwoord z.s.m. aan.
- Wachtwoorden verander je elk jaar.
- Je voert 'Clean-desk-policy'. Er zijn geen leerling gegevens openbaar toegankelijk in de school dus ook niet in jouw werkomgeving. Ook geen klassenlijst, lijst met telefoonnummers enz.
- Indien je ergens constateert dat dit wel het geval blijkt te zijn, handel je meteen om deze informatie af te schermen. Dus als je iets ziet bij je collega…., dan ga je er even heen.
- Je verlaat je werkplek niet zonder je digitale apparaten te vergrendelen, net zoals je papieren informatie ook opbergt. Op je PC kan dat eenvoudig met de combinatie van de **Windows-toets en L** (=Lock).
- USB-sticks worden binnen HSN niet meer gebruikt. Benodigde gegevens zijn immers altijd en overal beveiligd benaderbaar, omdat ze in alleen de cloud staan (Parnassys, Sharepoint).
- Voor HSN-zaken gebruik je HSN-mail – geen privé mail.
- Whatsapp en mail in klare taal is geen kanaal voor vertrouwelijke info
- HSN documenten en bijv. opgeslagen bijlagen bevinden zich in SharePoint – niet op thuis PC's.
- Er worden geen persoonsgegevens* op een apparaat opgeslagen. Indien noodzakelijk sla je tijdelijk op in de map Downloads. In Actanet wordt zo'n bestand na 8 dagen verwijderd. Thuis niet, daar zorg je dat je HSN bestanden zelf handmatig verwijdert. Daarna leeg je óók de prullenbak.
- Als je thuis werkt, doe je dat online in SharePoint, OneDrive, of Webmail.
- Je deelt geen leerlinggegevens* mondeling of schriftelijk of digitaal met derden. Alleen voor functioneel gebruik, met collega's, ouders en met daartoe bevoegde derden. Voor ál het andere delen (publiceren) van persoonsgegevens* is toestemming van de ouders nodig
- Je opent geen e-mail die 'vreemd oogt'. Je klikt ZEKER niet op een hyperlink dan.
  Het wordt een houding om, altíjd, vóór je klikt, onderin beeld te kijken waar de link wérkelijk heen gaat.
- Neem voor jezelf een e-mail-handtekening (hoe in te voegen)met bijvoorbeeld deze slotzin eronder: Is deze mail niet voor u bestemd, wilt u mij dan Beantwoorden en daarna deze mail verwijderen?
- Krijg je zelf een mail die niet voor jou bestemd is: beantwoord en verwijder deze.
- Een (vermoeden van) een datalek** meld je bij datalek@hsn-scholen.nl (privacy officer) en CC aan je directeur, je krijgt een aantal concrete vragen terug.

Deze notitie is af en toe geplaatst in Charisma's en elke nieuwe medewerker wordt naar AVG notities verwezen. Men moet schriftelijk te kennen geven dat men dit heeft gelezen en er mee akkoord gaat.

*** Persoonsgegeven**:
Elk gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Voor de hand liggende gegevens zijn iemands naam, adres en woonplaats. Maar ook telefoonnummers, postcodes met huisnummers, een foto, IP- of e-mailadres zijn persoonsgegevens. Gevoelige gegevens, over ras, godsdienst of gezondheid, worden bijzondere persoonsgegevens genoemd. Deze zijn door de wetgever extra beschermd (Autoriteit Persoonsgegevens). In de praktijk is iets al snel een persoonsgegeven.

**** Datalek of beveiligingsincident?**
Je raakt je laptop o.i.d. kwijt met leerlingdossiers. Is dit een datalek of een beveiligingsincident? In dit geval spreken we van een datalek. Het is belangrijk om het verschil te weten tussen een datalek en een beveiligingsincident.
We spreken van een **beveiligingsincident** als er iets gebeurt met informatie of informatiesystemen, waarbij de kans aanwezig is dat de vertrouwelijkheid, de integriteit of de beschikbaarheid hiervan in gevaar is, of kan komen.
Bij een **datalek** gaat het juist om een beveiligingsincident dat gevolgen heeft voor persoonsgegevens, waarbij de kans aanwezig is dat anderen zonder toestemming toegang hebben tot deze informatie. Het risico is dan groot dat zij deze informatie zomaar kunnen vernietigen, wijzigen of verspreiden. Denk bijvoorbeeld aan:

- het (per ongeluk) versturen van een e-mail met persoonsgegevens aan een verkeerde geadresseerde;
- het verliezen van een usb-stick, laptop, of telefoon met persoonsgegevens, zeker als dit apparaat niet goed beveiligd is;
- je wachtwoord raakt bekend;
- bij een vermoeden van een datalek.