Bijlage 1 Privacyreglement SOVON:
Protocol beveiligingsincidenten (waaronder datalekken)

Artikel 1. Doel van dit protocol

Het doel van dit protocol is tweeledig. Enerzijds dient het een personeelslid bewust te maken wat een inbreuk op de beveiliging is of kan zijn en anderzijds dient het personeelslid te informeren op welke wijze hij een mogelijk beveiligingsincident (dat mogelijk tevens een datalek blijkt te zijn) dient te signaleren.

Artikel 2. Begripsbepalingen

1.	personeel(slid):	iedere medewerker in loondienst van dan wel extern ingeschakeld door de SOVON en haar scholen;
2.	beveiligingsincident:	is een inbreuk op de beveiliging die mogelijk leidt tot het verlies of onrechtmatige verwerking van persoonsgegevens;
3.	datalek:	is een inbreuk op de beveiliging die wel leidt tot het verlies of onrechtmatige verwerking van persoonsgegevens;
4.	persoonsgegevens:	de gegevens als bedoeld in artikel 1 van het Privacyreglement;
5.	FG:	de Functionaris Gegevensbescherming, de heer I. Basoski, privacy@sovon.nu, 072-5671054.

Artikel 3. Meldplicht datalekken

Sinds 1 januari 2016 dient een verwerkingsverantwoordelijke (in dit geval de SOVON) een zogenaamd datalek onverwijld te melden aan de Autoriteit Persoonsgegevens (AP) en mogelijk ook aan de betrokkene(n) (in dit geval veelal het personeel of de <ouders en/of verzorgers van de> leerlingen. Van een datalek dat moet worden gemeld is sprake indien er persoonsgegevens verloren gaan of onrechtmatig worden verwerkt en het waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van betrokkene(n).

In het kader van deze wettelijke plicht heeft de SOVON dit protocol opgesteld en geïmplementeerd. Als de SOVON namelijk niet op de hoogte is van een mogelijk beveiligingsincident, kan zij haar wettelijke plicht niet vervullen. De SOVON is dan ook afhankelijk van de input die zij in dit verband krijgt van onder andere het personeel.

Artikel 4. Meldingsplicht personeel

Een personeelslid is verplicht een (mogelijk) beveiligingsincident dat hij/zij ontdekt direct per e-mail (privacy@sovon.nu) of telefonisch (072-5671054) te melden aan de FG, en/of aan zijn of haar direct leidinggevende ongeacht het tijdstip van de dag. Deze melding zal zo concreet mogelijk zijn. Het personeelslid neemt daarbij de inhoud van dit protocol in acht. Indien alleen gemeld aan de direct leidinggevende, is deze verplicht het (mogelijke) incident direct te melden bij de FG. Ook bij twijfel of er sprake is van een mogelijk beveiligingsincident, is het personeelslid verplicht dit te melden. Bij de melding (door personeelslid en/of direct leidinggevende) van een incident aan de FG legt de FG, in geval van een datalek, de relevante gegevens daarover in afstemming met de melder vast in het 'Formulier registratie datalekken SOVON' (bijlage 2 bij het Privacyreglement SOVON).

Artikel 5. Persoonsgegevens

Wat zijn persoonsgegevens? Dit zijn niet alleen gegevens zoals naam, adres, woonplaats of BSN-nummer. Deze gegevens worden aangeduid als direct identificerende gegevens. Daarnaast zijn er ook indirect identificerende gegevens. Dit zijn gegevens die iets zeggen over een natuurlijk persoon omdat zij gekoppeld kunnen worden aan een direct persoonsgegeven. Indien kan worden achterhaald om welke natuurlijke persoon het gaat, is er sprake van een persoonsgegeven. Het kan dus onder andere gaan om:

- naam;
- adres;
- telefoonnummer;
- e-mailadres;
- salarisgegevens;
- gegevens met betrekking tot ziekte;
- beoordelingsgesprekken;
- studieadviezen;
- gegevens met betrekking tot gezondheid;
- dyslexie of dyscalculie;
- betalingsachterstanden;
- gegevens over gezinssituatie;
- geloof;
- ras;
- studieresultaten;
- etc.

Artikel 6. Soorten beveiligingsincidenten

Er zijn verschillende soorten beveiligingsincidenten. Sommige beveiligingsincidenten zijn het gevolg van menselijke fouten, onoplettendheid of technisch falen. Deze beveiligingsincidenten worden niet bewust gecreëerd. Veel beveiligingsincidenten worden echter bewust gecreëerd.

Niet bewuste incidenten

Bij niet bewuste beveiligingsincidenten gaat het om incidenten die niet met opzet worden gecreeerd. Te denken valt aan:

- het laten liggen door van een laptop, tablet, smartphone of papieren dossier in de trein;
- het verliezen van een USB-stick, mobiele telefoon of bijvoorbeeld laptop;
- door haperende beveiliging (technische storing) zijn mogelijk persoonsgegevens van leerlingen ingezien door onbevoegden;
- de ruimte op school met daarin de fysieke leerlingendossiers heeft per ongeluk niet op slot gezeten voor een bepaalde periode;
- een docent heeft per ongeluk onbeheerd zijn laptop in de klas laten staan met daarop een memo-sticker met zijn inlognaam en wachtwoord;
- het verzenden door een medewerker van e-mail met vertrouwelijke gegevens aan de verkeerde ontvanger;
- het verzenden van een e-mail aan meerdere ontvangers die elkaars emailadressen niet kennen (zonder gebruik te maken van de bcc-optie);
- het crashen van een harde schijf met daarop persoonsgegevens;
- brand in een serverruimte of archiefruimte van de school;
- één van de hier voor genoemde situaties zich voordoet bij een verwerker van de school (bijvoorbeeld: de uitgever van digitale leermiddelen en Magister) voor zover het persoonsgegevens betreft van personeel of (ouder(s) en/of verzorger(s) van) leerlingen van de school.

Bewuste incidenten

Bij bewuste beveiligingsincidenten gaat het om incidenten die met opzet worden gecreëerd. Te denken valt aan:

- fysieke diefstal van een laptop, tablet, smartphone of (onderdelen van een) papieren dossier;
- het kopiëren, meenemen of bijvoorbeeld vernietigen van persoonsgegevens door personeel bijvoorbeeld uit onvrede over ontslag of studieadvies, als vriendendienst of als gevolg van chantage;
- phishing: het uitbuiten van menselijke kwetsbaarheden door hen onder valse voorwendselen persoonsgegevens te ontfutselen via mail of internet;
- hack: het uitbuiten van kwetsbaarheden in informatiesystemen en webservers;
- één van de hier voor genoemde situaties doet zich voor bij een bewerker van de school (bijvoorbeeld: de uitgever van digitale leermiddelen en Magister) voor zover het persoonsgegevens betreft van personeel of (ouder(s) en/of verzorger(s) van) leerlingen van de school.

Indien zich een dergelijk onbewust of bewust gecreëerd incident – of soortgelijkend incident – voordoet, is er sprake van een beveiligingsincident en dient het personeelslid dit te melden aan de FG en/of de direct leidinggevende. Indien gemeld aan de direct leidinggevende, dient deze het incident direct te melden aan de FG.