Bijlage 3 Privacyreglement SOVON:
Protocol voor het gebruik van e-mail, ICT en sociale media

Artikel 1 Werkingssfeer van deze regeling, begrippen

1.1 Deze regeling geeft de wijze aan waarop binnen de SOVON wordt omgegaan met informatie- en communicatietechnologie (hierna: ICT). Deze regeling omvat (gedrags)regels ten aanzien het gebruik van de ICT en geeft regels voor welke doeleinden en op welke wijze controle plaats vindt op dit gebruik. [1]

1.2 Deze regeling geldt voor eenieder die ten behoeve van de school werkzaamheden verricht (personeelsleden, maar bijvoorbeeld ook: stagiaires en vrijwilligers) of onderwijs volgt (leerlingen). Gezamenlijk worden zij in dit reglement ook aangeduid als 'gebruiker(s)'.

1.3 Elke nieuwe gebruiker wordt gewezen op de toepasselijkheid van deze regeling. Daarbij wordt aangegeven waar de volledige tekst van deze regeling geraadpleegd/ingezien kan worden. Alle personeelsleden en leerlingen ontvangen eens per jaar een herinnering aan de geldende regels.

1.4 Voor zover de gebruikers thuis of elders gebruik maken van de ICT (bijvoorbeeld het e-mailadres van de school of de schoolwebsite) zijn de bepalingen van deze regeling eveneens van toepassing.

Artikel 2 Toegang tot en gebruik van de ICT

2.1 De SOVON geeft de gebruiker het recht op toegang tot de ICT (en de daarmee verbonden systemen en faciliteiten), maar behoudt zich het recht voor de toegang weer in te trekken.

2.2 Gebruikersidentificatie (gebruikersnaam) en authenticatie (wachtwoord) worden door de ICT-afdeling verstrekt en zijn persoonsgebonden en mogen niet aan anderen worden doorgegeven.

2.3 Het is gebruiker niet toegestaan om persoonsgegevens die gebruiker ter beschikking staan voor de uitoefening van zijn functie lokaal op te slaan (dus niet op het computernetwerk) noch op privé-apparatuur, tenzij daarvoor voorafgaande toestemming is verleend door diens leidinggevende en adequate waarborgen zijn getroffen voor de beveiliging van de persoonsgegevens. [2]

---

[1] Opties voor aanvullingen op dit protocol: zie https://www.sambo-ict.nl/wp-content/uploads/2017/10/IBPDOC26-Verantwoord-netwerk-gebruik-2.0.docx

[2] Met het oog op de beveiliging van persoonsgegevens dient de school een afweging te maken over de mogelijkheden en beperkingen in het gebruik van persoonlijke mobiele apparaten door leraren en leerlingen binnen de school. Zie ook de brochure 'Bring Your Own Device? Hoe? Zo!', kennisnet juni 2013,www.sambo-ict.nl/wp-content/uploads/2013/06/HoeZo-Bring-Your-Own-Device.pdf)

Artikel 3 Gebruik van de ICT-apparatuur

3.1 De gebruiker dient zorgvuldig om te gaan met de ICT-apparatuur, zodat deze niet beschadigd raakt. De apparatuur dient in goede orde te worden achtergelaten. Eventuele schade of ontbreken van onderdelen dient direct gemeld te worden aan de ICT-afdeling.

3.2 Alleen de ICT-afdeling is bevoegd om apparatuur te ontkoppelen, verplaatsen of aan te sluiten aan het schoolnetwerk of aan apparatuur die aan het schoolnetwerk verbonden is.

3.3 De ICT-afdeling verleent alleen ondersteuning op apparatuur die door de ICT-afdeling is aangeschaft, aangesloten en geïnstalleerd.

3.4 Het gebruik van eigen opslagmedia (bijvoorbeeld: een USB-stick) van de gebruikers is toegestaan, onder de volgende voorwaarden:

a) voor het correct laten functioneren van het opslagmedium kan geen beroep worden gedaan op de ICT-afdeling;

b) de bestanden en programmatuur die op het opslagmedium staan moeten voldoen aan de voorwaarden zoals vastgelegd in dit reglement.

3.5 Het gebruik van eigen computerapparatuur (bijvoorbeeld laptops of tablets) is toegestaan onder de volgende voorwaarden:

a) voorafgaand aan het gebruik is toestemming verleend door de leidinggevende en is contact opgenomen met de ICT-afdeling. Deze is bevoegd om, met opgaaf van redenen, de apparatuur niet toe te staan;

b) de gebruiker geeft de ICT-afdeling de gelegenheid om voorafgaand aan het gebruik maatregelen te treffen om de beheersbaarheid en de veiligheid te waarborgen;

c) het gebruik van de betreffende apparatuur moet voldoen aan de voorwaarden zoals vastgelegd in dit reglement.

Artikel 4 Toegang tot en gebruik van internet en e-mail

4.1 De SOVON behoudt zich het recht voor om de toegang tot bepaalde sites door middel van een filtersysteem te beperken.

4.2 Het versturen van e-mailberichten moet voldoen aan de volgende algemene voorwaarden:

a) de afzender wordt correct weergegeven;

b) duidelijke onderwerp aanduiding;

c) terughoudend omgaan met vertrouwelijke gegevens en gevoelige informatie.

4.3 Voor het verzenden en ontvangen van e-mail binnen de school wordt alleen gebruik gemaakt van de e-mailprogrammatuur die de school hiervoor beschikbaar stelt. Het gebruik van andere mailprogrammatuur is niet toegestaan.

4.4 Omdat het verzenden van gegevens met gebruikmaking van Gmail, Hotmail, Dropbox, Whatsapp en WeTransfer leidt, dan wel kan leiden, tot doorgifte van Persoonsgegevens bui-

ten de EER, hetgeen slechts is toegestaan onder voorwaarden, kan de SOVON – indien door haar niet langer aan deze voorwaarden kan worden voldaan - besluiten het gebruik van deze software door medewerkers te verbieden.

Artikel 5 (On)verantwoord gebruik van de ICT

Verantwoord gebruik

5.1 Het gebruik van de ICT is primair verbonden met taken en bezigheden die voortvloeien uit het verstrekken of ontvangen van onderwijs en begeleiding. Als uitgangspunt geldt dat het gebruik van de ICT van de school ten dienste moet staan aan de werkzaamheden van het personeelslid of de opleiding van de leerling. Indien en voor zover sprake is van het verwerken van persoonsgegevens gebeurt dit met inachtneming van het Privacyreglement.

5.2 Personeelsleden mogen de ICT beperkt, incidenteel en kortstondig gebruiken voor persoonlijke doeleinden, mits dit niet storend is voor de dagelijkse werkzaamheden of het systeem en mits hierbij wordt voldaan aan de verdere regels van deze regeling. Leerlingen mogen de ICT onder schooltijd in principe niet voor persoonlijke doeleinden gebruiken, tenzij zij daarvoor toestemming hebben gekregen.

5.3 Gebruikers van de ICT systemen worden opgeroepen melden gesignaleerde zwakke plekken in de systemen, zodat zo snel mogelijk maatregelen kunnen worden getroffen. Melding kan worden gedaan bij de Functionaris Gegevensbescherming, via privacy@sovon.nu.

Onverantwoord gebruik

5.4 Het is niet toegestaan om de ICT zodanig te gebruiken dat het systeem- en/of de beveiliging opzettelijk worden aangetast.

5.5 Het is niet toegestaan zich toegang te verschaffen tot gegevens van andere gebruikers, tenzij met uitdrukkelijke toestemming van de betreffende gebruiker.

5.6 Het is niet toegestaan pogingen te ondernemen om het filtersysteem te omzeilen.

5.7 Het is in het bijzonder niet toegestaan om:

a) sites te bezoeken die pornografisch, racistisch, discriminerend, (seksueel) intimiderend, beledigend of aanstootgevend materiaal bevatten;

b) pornografisch, racistisch, discriminerend, (seksueel intimiderend, beledigend of aanstootgevend materiaal te bekijken of te downloaden of te verspreiden;

c) zich tot niet-openbare bronnen op het netwerk, internet of andere computernetwerken toegang te verschaffen en het bewust informatie waartoe men via de ICT oneigenlijk toegang heeft verkregen zonder toestemming te veranderen of te vernietigen;

d) bestanden te downloaden en/of op het computernetwerk of lokaal op een PC van de school te plaatsen die geen verband houden met studie en/of werk;

e) software en applicaties te downloaden en/of te installeren zonder voorafgaande toestemming van de ICT-afdeling;
f) niet-educatieve spelletjes te spelen;
g) anoniem of onder een fictieve naam via de ICT te communiceren;
h) op dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende manier via de ICT te communiceren;
i) inkomende privé-berichten te genereren door het deelnemen aan niet-zakelijke nieuwsgroepen, abonnementen op e-zines, elektronisch winkelen, down- en uploaden van bestanden, nieuwsbrieven en dergelijke;
j) kettingmailberichten en andere berichten die verstopping veroorzaken of het werk van anderen verstoren te verzenden of door te sturen;
k) iemand lastig te vallen via de ICT;
l) het introduceren en verspreiden van computervirussen en andere software die de integriteit van de gegevens of de computerbeveiliging van de ICT kunnen beschadigen;
m) gebruik te maken van MSN Messenger en andere chatvoorzieningen.

5.8 Het is niet toegestaan om foto's, video's of ander materiaal van op school werkzame personen of leerlingen of andere bij de school betrokkenen via de ICT (daaronder ook begrepen: social media) te publiceren, tenzij dit gericht is op een aan het onderwijs gerelateerde doelstelling en de afgebeelde personen hebben aangegeven in te stemmen met dergelijke publicaties.

5.9 Het is ook anderszins niet toegestaan om door middel van de ICT in strijd met de wet of onethisch te handelen.

5.10 De schoolleiding kan de ICT-afdeling opdracht geven geconstateerde ongeoorloofde data van het computernetwerk te verwijderen.

5.11 Voor personeelsleden is het voor testdoeleinden toegestaan software lokaal te installeren die nodig is voor de werkzaamheden ten behoeve van school, mits met toestemming van de ICT-afdeling.

5.12 Een vermoeden van misbruik van ICT en inbreuken op de beveiliging, van binnenuit of van buiten de school dienen onmiddellijk aan de ICT-afdeling gemeld te worden, hieronder vallen tevens inbreuken op de beveiliging die bij toeval worden ontdekt.

5.13 Als de gebruiker eraan twijfelt of een bepaald gebruik van ICT wel verantwoord is, dan overlegt hij daarover met de ICT-afdeling.

Artikel 6 Algemene uitgangspunten van controle op gebruik

6.1 De schoolleiding heeft er recht op en belang bij dat zij het gebruik van de ICT door personeelsleden en leerlingen kan controleren. De controle op gebruik van de ICT zal overeenkomstig deze regeling uitgevoerd worden. Als zich situaties voordoen waarin deze regeling niet voorziet, dan zal conform de Algemene Verordening Gegevensbescherming (AVG) gehandeld worden.

6.2 Als een directielid merkt of erop geattendeerd wordt dat het ICT-gedrag van een personeelslid niet binnen de kaders van dit reglement verloopt, wordt het personeelslid hierop door het directielid gewezen en wordt een controle van zijn ICT-gebruik door bevoegde personen van de ICT-afdeling als mogelijkheid genoemd. Het directielid meldt dit aan de locatiedirecteur of de centrale directie.

6.3 Als een personeelslid merkt dat het ICT-gedrag van een leerling niet binnen de kaders van dit reglement verloopt, dan spreekt het personeelslid deze leerling hierop aan en meldt dit aan het locatiedirectielid waaronder deze leerling resorteert.

6.4 Gestreefd wordt naar een goede balans tussen enerzijds controle op het gebruik van de ICT en anderzijds de bescherming van de privacy van personeelsleden en leerlingen.

6.5 Controle op het gebruik van de ICT zal waar mogelijk zoveel mogelijk geautomatiseerd plaatsvinden, waarbij in geval van verdachte berichten, het bericht geautomatiseerd wordt teruggezonden aan de verzender. Voor zover geautomatiseerde controle niet mogelijk, dan wel ontoereikend is, zal de controle op het gebruik van de ICT in beginsel steekproefsgewijs plaatsvinden.

6.6 In geval dat ten aanzien van een gebruiker, vanwege een concreet vermoeden van oneigenlijk gebruik, een gerichte controle is uitgevoerd, stelt de schoolleiding deze gebruiker daarvan zo spoedig mogelijk nadat de controle heeft plaatsgevonden van op de hoogte.

6.7 Persoonsgegevens met betrekking tot het gebruik van ICT worden niet langer bewaard dan noodzakelijk, met een bewaartermijn van [maximaal 6 maanden]. Onder omstandigheden kan een langere bewaartermijn gerechtvaardigd zijn. In dat geval zal de verwerking worden gemeld bij de Autoriteit Persoonsgegevens.

6.8 Privémail/-gebruik (voorzien van het label ‘persoonlijk’) wordt zoveel mogelijk ontzien van controle.

6.9 Elektronische informatie- en communicatieberichten van vertrouwenspersonen en andere personeelsleden met een vertrouwensfunctie, gecommuniceerd in het kader van hun functie, zijn uitgesloten van inhoudelijke controle.

6.10 De schoolleiding treft voorzieningen voor de positie en de integriteit van de ICT-afdeling. De medewerkers van de ICT-afdeling hebben een geheimhoudingsplicht die inhoudt dat ten aanzien van de verzamelde en voor hen inzichtelijke informatie strikte geheimhouding betracht dient te worden.

Artikel 7 Doeleinden van controle

7.1 De controle op persoonsgegevens bij gebruik van de ICT vindt slechts plaats met als doel:
- a) het tegengaan van onverantwoord en ontoelaatbaar gebruik;
- b) de naleving van het Privacyreglement;
- c) het bewaken van de voortgang van werkzaamheden;
- d) het vastleggen van bewijs en/of archief;
- e) de systeem- en netwerkbeveiliging;
- f) de kosten- en capaciteitsbeheersing.

7.2 Onder 'onverantwoord en ontoelaatbaar gebruik' als bedoeld in artikel 7.1 wordt begrepen: het onverantwoord gebruik als opgenomen in artikel 5.4 tot en met 5.13.

7.3 Onder 'bewaking van de voortgang van de werkzaamheden' als bedoeld in artikel 7.1 wordt begrepen: controle op de inhoud van zakelijke e-mails van personeelsleden voor wie het communiceren per e-mail rechtstreeks met de te verrichten taken verband houdt. Middels deze controle kan de voortgang van de werkzaamheden worden gegarandeerd bij ziekte of afwezigheid van de medewerker.

7.4 Onder 'vastleggen van bewijs en/of archief' als bedoeld in artikel 7.1 wordt begrepen: het maken van kopieën van e-mails vanuit de behoefte aan bewijs voor zakelijke transacties en dossiervorming (al dan niet met het oog op het voeren van juridische procedures).

7.5 Onder 'systeem- en netwerkbeveiliging' als bedoeld in artikel 7.1 wordt begrepen: controle op het e-mail- en internetgebruik ter voorkoming van systeemaanvallen door onder andere virussen, trojans of andere schadelijke programma's.

7.6 Onder 'kosten- en capaciteitsbeheersing' als bedoeld in artikel 7.1 wordt begrepen: controle op het e-mail- en internetgebruik ter inventarisering en/of beheersing van de kosten die gemoeid zijn met het gebruik van de ICT.

Artikel 8 Specifieke uitgangspunten van controle op gebruik

8.1 In het kader van de controle op de gebruikers voor het doel als bedoeld in artikel 7.1a geldt dat:
- a) controle op de naleving van de regels vindt in beginsel geautomatiseerd en steekproefsgewijs plaats;
- b) indien er een concreet vermoeden is dat een gebruiker de regels, waarvan de naleving wordt gecontroleerd, overtreedt, vindt zo nodig een in tijd en omvang zo beperkt mogelijke gerichte controle op persoonsniveau plaats;
- c) daarbij worden in eerste instantie de berichten en/of het surfgedrag gescreend op (onder andere) verdachte afzender(s), bestemming, website, verdacht onderwerp, verdachte zoekopdracht, verboden woord in de inhoud of verboden extensies van de bijlage(n);

d) vervolgens worden de berichten, waarvan aannemelijk is dat het regulier verkeer betreft of waartegen ook overigens geen bedenkingen bestaan, ongeopend doorgezonden (bij originelen) of vernietigd (kopieën);
e) de overgebleven berichten kunnen worden geopend voor nader inhoudelijk onderzoek.

8.2 In het kader van de controle voor het doel als bedoeld in artikel 7.1 b geldt dat slechts berichten worden verwerkt die rechtstreeks verband houden met uitvoering van de te verrichten taken door het personeelslid.

8.3 In het kader van de controle voor het doel als bedoeld in artikel 7.1 c geldt dat slechts de e-mailverkeersgegevens en inhoud van de berichten wordt verwerkt.

8.4 In het kader van de controle voor het doel als bedoeld in artikel 7.1 d geldt dat slechts zakelijke berichten worden verwerkt voor zover deze kunnen dienen als bewijs van zakelijke transacties en dossiervorming.

8.5 In het kader van de controle voor het doel als bedoeld in artikel 7.1 e geldt dat:
a) de controle geheel geautomatiseerd plaatsvindt;
b) een gevonden besmet bericht/bestand op een aparte locatie bewaard wordt voor nader onderzoek en eventuele herstelwerkzaamheden.

8.6 In het kader van de controle voor het doel als bedoeld in artikel 7.1 e geldt dat slechts de
a) e-mailverkeersgegevens en inhoud (en bijlagen) van berichten met een verdachte inhoud worden gecontroleerd;
b) internetverkeersgegevens en inhoud van berichten met een verdachte inhoud worden gecontroleerd.

8.7 In het kader van de controle voor het doel als bedoeld in artikel 7.1 f geldt dat de controle van het e-mail- en internetverkeer beperkt blijft tot de verkeersgegevens.

8.8 In het kader van de controle voor het doel als bedoeld in artikel 7.1 f geldt dat slechts de
a) e-mailverkeersgegevens over tijd, hoeveelheid, omvang en dergelijke worden verwerkt;
b) internetverkeersgegevens over tijd en dergelijke worden verwerkt.

Artikel 9 Gebruik van social media

9.1 Onder social media worden verstaan alle huidige en toekomstige online platforms waarbij de gebruikers de inhoud verzorgen.

9.2 Indien social media voor onderwijsdoeleinden worden gebruikt dient dit – met het oog op de bescherming van leerlinggegevens - plaats te vinden conform het Privacyreglement.

9.3 Voor het overig gebruik geldt dat dit in eigen tijd dient plaats te vinden. Dat geldt ook voor het gebruik van social media door middel van smartphones of tablets.

9.4 Voor zover de gebruikers (leerlingen, personeelsleden of derden) aan de school verbonden zijn, geldt in algemene zin dat zich niet op social media zullen uitlaten op een wijze die schadelijk kan zijn voor de school en/of de SOVON.

9.5 De SOVON kan het gebruik van specifieke social media door medewerkers verbieden, indien dit (gebruik) risico's oplevert voor de privacy van leerlingen en/of medewerkers.

Artikel 10 Richtlijnen voor het gebruik van social media

10.1 Voor zover de gebruiker op social media-uitingen doet die in relatie staan tot de SOVON en/of een of meer van de tot de SOVON berhorende scholen geeft hij steeds duidelijk aan in welke relatie (bijvoorbeeld: personeelslid of leerling) hij staat tot de SOVON en/of betreffende school of scholen.

10.2 De gebruiker plaatst op social media geen content met een onverantwoorde inhoud.

10.3 De gebruiker deelt op social media geen interne- of bedrijfsvertrouwelijke informatie over de SOVON of tot de SOVON behorende scholen.

10.4 De gebruiker deelt geen persoonsgegevens van personeel of leerlingen waartoe hij uit hoofde van zijn functie toegang heeft.

10.5 De gebruiker laat zich op social media niet negatief of anderszins ongepast uit over de SOVON, over scholen behorend tot de SOVON, over collega's, over personeelsleden en/of over (mede-)leerlingen.

10.6 De gebruiker plaatst op social media niet zonder toestemming foto's of andere afbeeldingen van de SOVON en/of tot de SOVON behorende scholen en/of aan de SOVON en/of aan daartoe behorende scholen verbonden personen.

10.7 De gebruiker plaatst op social media geen content namens de SOVON, tenzij hij daarvoor toestemming heeft gekregen.

10.8 In zijn algemeenheid geldt dat de gebruiker op social media geen content zal plaatsen of zich anderszins zal gedragen op een wijze die de SOVON en/of tot de SOVON behorende scholen schade kan toebrengen.

Artikel 11 Richtlijnen voor contact middels ICT

11.1 Privé-contact tussen personeelsleden en leerlingen, binnen dan wel buiten schooltijd, door middel van e-mail en smartphones (bijvoorbeeld via Whatsapp) is in beginsel verboden.

11.2 Een uitzondering kan aan de orde zijn ten aanzien van leerlingen die speciale begeleiding op afstand nodig hebben, bijvoorbeeld in geval van ziekte. Een dergelijk contact mag alleen betrekking hebben op onderwijsgerelateerde zaken (bijvoorbeeld kennisoverdracht, afstemming huiswerk, ondersteuning) en dient vooraf gemeld te zijn bij de leidinggevende. Het personeelslid mag het contact met de leerling uitsluitend onderhouden via het e-mailadres van de school.

11.3 Onderling contact tussen personeelsleden over een leerling is uitsluitend toegestaan in verband met onderwijsgerelateerde zaken en mag uitsluitend verlopen via het e-mailadres van de school.

11.4 Het is personeelsleden niet toegestaan persoonsgegevens van leerlingen op te slaan op servers die niet worden gebruikt of beheerd door de school of lokaal op de eigen PC respectievelijk tablet of smartphone.

11.5 Gewisselde (e-mail)correspondentie wordt maandelijks door de betrokken docenten vernietigd dan wel – indien de informatie relevant is voor de begeleiding van de leerling - verplaatst en opgeslagen in het leerlingvolgsysteem van de SOVON.

Artikel 12 Disciplinaire maatregelen bij leerlingen

12.1 Indien door de schoolleiding wordt vastgesteld dat een leerling onverantwoord gebruik heeft gemaakt van de ICT, kan de schoolleiding – afhankelijk van de aard en de ernst van het onverantwoorde gebruik – overgaan tot:

a) het tijdelijk uitsluiten van inlogmogelijkheden voor de betrokken leerling;
b) het melden van dit gedrag en de consequenties aan de ouder(s)/verzorger(s); en/of
c) het opleggen van een straf/maatregel en/of het daartoe voordragen van de leerling bij het bestuur van de SOVON (in geval van een verwijdering).

Artikel 13 Disciplinaire maatregelen bij personeelsleden

Indien door de schoolleiding wordt vastgesteld dat een personeelslid onverantwoord gebruik heeft gemaakt van de ICT, kan de schoolleiding - afhankelijk van de aard en de ernst van het onverantwoorde gebruik – maatregelen treffen, zoals een berisping, schorsing of ontslag.