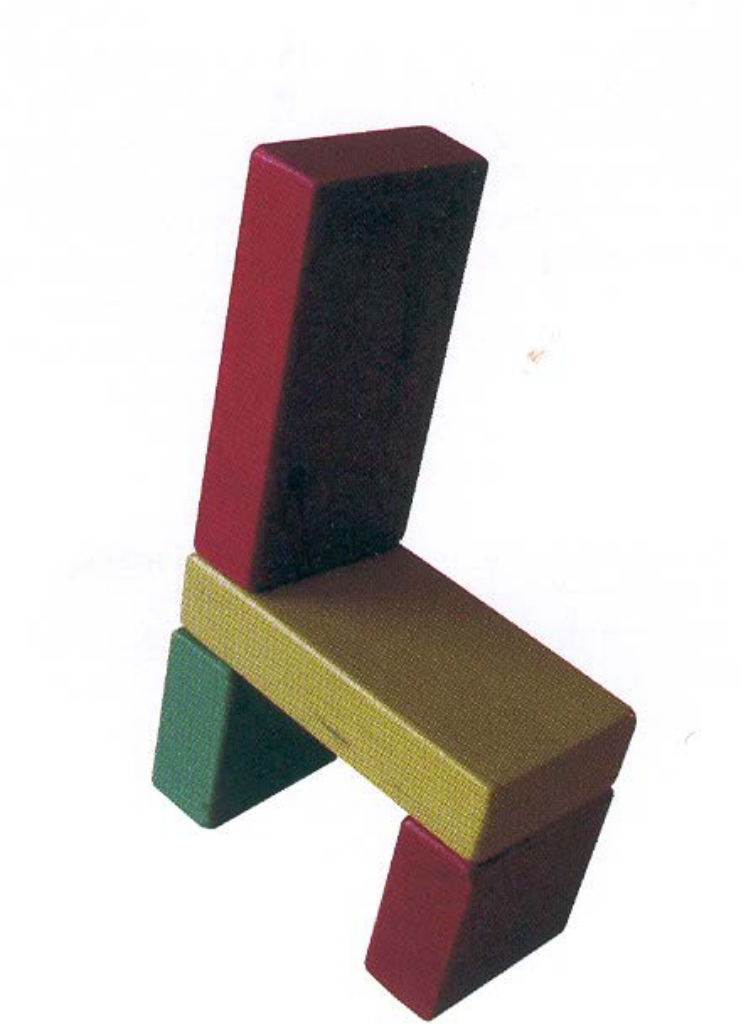
2018

NBS De Hoogakker

Serge van Meer, Kees van der Plas



[*Veilig omgaan met digitale commucicatiemiddelen*]

Hoe gaat de Hoogakker om met digitale communicatiemiddelen ten opzichte van leerlingen, personeel, ouders en de maatschappij?

Inhoud

1. Internet

Het Internet is een wereldwijd samenstel van tienduizenden computers en computernetwerken, zonder centrale controle of eigenaar. Een onbegrensde informatiebron en tegelijk ook communicatiemedium.

Belangrijke onderdelen zijn:

- Het World Wide Web (de webpagina's)
- E-mail (elektronisch berichtenverkeer)
- Allerlei sociale media platformen:
  - WhatsApp
  - Instagram
  - YouTube
  - Snapchat
  - Facebook

Op het internet gelden er geen beperkingen over het soort informatie dat beschikbaar wordt gesteld. De meeste Internetgebruikers hebben positieve ervaringen met Internet. Maar, net zoals in elke samenleving, zijn er wat risico's. Het Internet kent, zoals de "gewone" samenleving, de meest uiteenlopende bewoners. De meeste zijn welgemanierd en netjes. Maar er zijn helaas enkele negatieve uitzonderingen.

2. Wat zijn de risico's?

- Niet alle plaatsen op het internet zijn geschikt voor kinderogen. Ongewenst is niet alleen pornografie, maar ook teksten of foto's die betrekking hebben op bijvoorbeeld extreem geweld, racisme of extremisme.
- Sommige sites hebben een onvolledige, misleidende of foutieve inhoud.
- Als kinderen persoonlijke informatie doorgeven via chatten of e-mail, kan dit leiden tot schadelijke contacten. Pedofielen doen zich bijvoorbeeld op het internet soms voor als kinderen en proberen een afspraakje in de echte wereld te maken. (Grooming)
- Bij het verspreiden of delen van seksueel getinte foto's of berichten via mobiele telefoons of andere mobiele media ben je niet alleen aan het pesten, maar dit is zelfs strafbaar. (Sexting)
- Als een bericht wordt verstuurd, kan het gevolg zijn dat er heel veel ongewenste reclame terug ontvangen wordt. (Spam)
- Digitale aankopen kunnen vervelende consequenties hebben.
- Door het min of meer anonieme karakter van het internet lokt het medium, met name bij e-mail en chatapps, uit tot het gebruik van grof of kwetsend taalgebruik.
- Het publiceren van materiaal op het internet, dat auteursrechterlijk beschermd is, kan beboet worden. Ook het illegaal downloaden van software, muziek, etc. van peer-to-peer sites zoals uTorrent, Bittorent, Soulseek, Shareaza, eMule e.d. is strafbaar.
- Het is ook mogelijk via internet virussen binnen te krijgen. Met name de e-mail virussen vormen een groot risico. Ook andere externe opslag devices kunnen een virus overdragen.
- Computer inbraak (hacken) door kwaadwilligen is een veel voorkomend risico.

3. Wat kan de school doen om risico's te beperken?

Hieronder wordt beschreven wat de school zoal kan doen om de risico's te beperken.

Men kan heel wat maatregelen treffen. Het is echter onmogelijk en soms onwenselijk alle risico's uit te sluiten. Als school dient er overleg met alle geledingen (Bestuur, MR, team, etc.) te zijn om te komen tot verantwoorde keuzes, die passen bij de filosofie, visie, identiteit en regelgeving van de school.

3.a.Technisch: Hackers, Virussen en Passwords

3.a.1. Algemeen:

Hackers zijn personen die met behulp van een computerprogramma inbreken in een computer of het netwerk van een ander met als doel schade toe te brengen in het netwerk of gegevens uit het netwerk te ontvreemden. Deze vorm van braak is alleen mogelijk als men is verbonden met het internet.
De virusmakers proberen telkens weer virussen te bedenken die een bedreiging voor de netwerken vormen. Iedereen heeft daar last van en wij als school dus ook. Naast virussen is spam ook een toenemend probleem.
Het is ook belangrijk goede passwords te gebruiken om het hackers moeilijker te maken.

3.a.2. Maatregelen:

- Met behulp van een zgn. firewall en een goed antivirusprogramma kan men zich relatief eenvoudig beschermen tegen hackers en virussen.
  Een firewall zorgt ervoor dat hackers geen toegang meer hebben tot het schoolnetwerk.
  Op de scholen van de SNB zijn degelijk beproefde firewalls van Cisco (=marktleider in firewalloplossingen) geplaatst.
- De aanschaf en het onderhouden van een anti-virusprogramma is een absolute noodzaak! Een goed antivirus programma wordt indien nodig dagelijks bijgewerkt door de makers ervan. Gebruikers kunnen updates via het internet binnenhalen.
- Passwords dienen iedere veertig dagen gewijzigd te worden. Dienen meer dan 8 karakters en verschillende tekens te bevatten.

3.a.3. Hoe gaan we met calamiteiten/aanvallen om?

Bij geconstateerde inbraken en virusaanvallen wordt alles in het werk gesteld om de schade te beperken en eventuele bronnen van aanvallers te herleiden. Door backups zal verloren of aangetaste data teruggezet worden.

3.a.4. Wie grijpt in?

De ICT coördinator zal samen met de technici van VDN de juiste acties ondernemen om het probleem op te lossen. Aan de directeur zal worden gerapporteerd.

3.b. Begeleidend confronteren: Het gebruik van het world wide web en sociale media

3.b.1. Algemeen:

Veilig gebruik van het internet en sociale media is een faciliteit die alle leerlingen onder de knie moet krijgen. Daarbij is het gewenst om de strategie van het “begeleidend confronteren” toe te passen. “Begeleidend confronteren” houdt in dat men kinderen leert omgaan met internet en sociale media, zoals het is. Het is een afspiegeling van de maatschappij. Net als in de maatschappij moeten kinderen leren wat goed is en wat niet goed is, wat kan en wat niet kan. Zoals ze geleerd wordt om te gaan met televisie en druk verkeer, zo moet dat ook met het internet en sociale media: onder begeleiding en stapje voor stapje. Bespreek met kinderen de ins en outs van het internet en sociale media.

3.b.2. Voorwaarden:

De veiligste manier om kinderen gebruik te laten maken van internet en sociale media is door hen te begeleiden, door je eigen kennis op dit gebied te vergroten en door kinderen op te voeden naar de normen en waarden, die op je school gelden.
Heel belangrijk is het dat leerkrachten zelf mediawijs genoeg zijn. Leerkrachten moeten kunnen surfen (o.a. omgaan met zoekmachines), e-mailen, chatten en bekend zijn met allerlei sociale media platformen (Instagram, Facebook, YouTube…) De school biedt de leerkracht de mogelijkheid om zich te kunnen scholen middels de ICT Academie. (Deskundigheidsbevordering op ICT gebied voor leerkrachten van de SNB dóór leerkrachten van de SNB). Door ICT vergaderpunten op de Bouwvergaderingen te plaatsen komen eventuele leervragen aan bod waar meteen adequate actie mbt deskundigheidsbevordering op gezet kan worden. Leerkrachten van de groepen 5 t/m 8 beschikken over de lesmethode Mediawijs met Kidsweek in de klas, die uitgaat van de tien mediawijsheidcompetenties (mediawijzer.nl)

Docenten moeten zich bewust zijn van de mogelijke risico’s, die internetgebruik en sociale media platformen met zich meebrengen.

Er dient voor gezorgd te worden dat kinderen positieve ervaringen krijgen. De verrichtingen van de kinderen dient gevolgd te blijven worden. Laat de kinderen tonen wat ze hebben gedaan op Internet en kijk mee met wat ze doen op de verschillende sociale media platformen. Kinderen mogen zonder toestemming het internet op school niet bezoeken.

Het principe van achteraf filteren (dit is ook mogelijk op de server) door achteraf na te gaan waar leerlingen zijn geweest, is mogelijk. Wenselijk is het met kinderen af te spreken welke sancties volgen bij het overtreden van de vast gestelde internetregels.[kvdp1]

3.b.3. Gebruiksvoorwaarden/nettiquette (etiquette voor internetgebruik en sociale media)

Op school zijn met personeel en leerlingen de volgende gebruikersvoorwaarden afgesproken:

De volgende zaken zijn niet gewenst:

- Internet sites bezoeken die obscene, tot haat opruiende of anderszins aanstootgevende informatie bevatten. Obscene of lasterlijke informatie of informatie die tot doel heeft andere personen te ergeren, kwellen of intimideren, verzenden of ontvangen.
- In discussie gaan over school/organisatie gerelateerde onderwerpen middels sociale media.
- Tijd besteden aan zaken die geen verband houden niets te maken hebben met het onderwijs of de instelling.
- Door e-mailberichten reacties uitlokken die geen verband houden en niets te maken hebben met de activiteiten van de school.
- Je persoonlijke mening als de mening van de school voorstellen.
- Het Internet of e-mail gebruiken voor gokken of onwettige activiteiten.
- Ontoelaatbare opmerkingen, voorstellen of materialen vervaardigen of op het Internet plaatsen.
- Commerciële software of materiaal waarop copyright berust in strijd met dat copyright uploaden, downloaden of anderszins overbrengen.
- Software of computerbestanden downloaden zonder de maatregelen voor bescherming tegen virussen te nemen die door de leiding van de instelling zijn goedgekeurd of voorgeschreven.
- De normale werking van het netwerk opzettelijk verstoren, waaronder tevens wordt verstaan het verspreiden van computervirussen of van netwerkverkeer van grote omvang over langere tijd, waardoor anderen wezenlijk worden gehinderd bij hun gebruik van het netwerk.
- Vertrouwelijke informatie of informatie die eigendom is van personen of instellingen bekend maken, publiceren of onbeheerd achterlaten. Dergelijke informatie bestaat onder meer uit, maar is niet beperkt tot: databases van de instelling en de daarin opgeslagen gegevens, computersoftware, toegangscodes voor computernetwerken en persoonlijke gegevens van leerlingen. De computer niet vergrendeld achterlaten.
- Medewerkers van de school publiceren of delen geen vertrouwelijke informatie (waaronder persoonsgegevens van bij de organisatie betrokken personen zoals medewerkers, leerlingen en ouders en extern betrokkenen) op sociale media
- Zonder uitdrukkelijke toestemming van de eigenaar bestanden, uitvoer of gebruikersnamen van andere personen openen, wijzigen of gebruiken.
- Ander gebruik van het Internet of van netwerkbronnen dat door de leiding van de instelling of de netwerkbeheerder als niet passend bij de algemeen aanvaarde normen en waarden wordt aangemerkt.

We gaan bewust om met wat we delen: Is het wel of niet verstandig te publiceren, wat zijn de eventuele consequenties en is het betreffende sociale platform/middel wel het meest geschikt voor de te delen inhoud

3.b.4. Acht Gouden Mediawijsheid regels voor kinderen (internet en sociale media protocol)

1. Ik mag alleen mijn voornaam gebruiken. Ik geef anderen geen persoonlijke gegevens zoals mijn adres, mijn telefoonnummer, mijn email-adres of het adres van mijn ouders of van andere bekenden.
2. Ik zal nooit toestemming geven aan iemand, die ik op internet of sociale media platformen ben tegengekomen in het echt te ontmoeten.
3. Ik zal deze 'onbekende personen' geen foto's van mezelf of anderen toesturen, behalve als mijn ouders en/of mijn leerkracht hier toestemming voor hebben gegeven.
4. Ik plaats, verstuur en reageer niet op gemene, valse, vervelende berichten en seksueel getint beeldmateriaal van mijzelf of andere mensen.
5. Ik ga meteen naar de meneer, juf of mijn ouders als ik hele vervelende informatie tegenkom. Zij kunnen eventueel contact opnemen met de politie.
6. Als ik een sociaal media platform mailserver gebruik om met anderen te communiceren, zal ik me netjes gedragen. Mijn taalgebruik is immers een goede reclame voor mijzelf en voor onze school. Digitale communicatie onder schooltijd mag niet, mits ik toestemming heb van de leerkracht.
7. Ik geloof niet alles wat ik te zien en te lezen krijg op internet.
8. Op school gebruik ik alleen de hardware en software waar ik toestemming voor heb en zorg ik ervoor dat ik met alles zorgvuldig omga. Mocht ik iets verkeerds hebben gedaan, meld ik dit meteen bij de leerkracht.

3.c. E-mail

3.c.1. Algemeen

Ieder personeelslid heeft een zakelijk e-mailadres. Hiermee wordt gecommuniceerd naar alle onderwijs gerelateerde mensen. Leerlingen vormen hierop een uitzondering. Om met leerlingen te communiceren is onze VLE My Learning het aangewezen middel.

3.c.2. Afspraken

a. Werknemers mogen hun SNB mailbox gebruiken voor alle mail die werk gerelateerd is.
b. We verwachten van onze medewerkers dat ze werk gerelateerde mail alleen via dit mailadres versturen en niet via privé mailboxen.
c. Hoog privacy gevoelige informatie wordt op een zo veilig mogelijke manier uitgewisseld, met in achtneming van de vijf vuistregels. Als via de mail bijlages (met hoog privacy gevoelige inhoud) verstuurd worden, worden deze bij voorkeur beveiligd verstuurd. Beveiligingscode/sleutel kan los naar de ontvanger gestuurd worden zodat alleen hij of zij de inhoud zichtbaar kan maken.
d. De mailbox is niet bedoeld als archief voor bijvoorbeeld via de mail ontvangen bijlages. Sla deze altijd op
op de daar voor bedoeld opslagomgevingen. (zie punt 3.4 van dit document)
e. Bij mail verstuurd naar grote groepen personen gebruiken we bij voorkeur de BCC mailfunctie. Voor intern delen van documenten gebruiken we My Learning en geen e-mail.
f. De optie 'allen beantwoorden' gebruiken we alleen indien de noodzaak daarvoor aanwezig is.

g. Niemand mag, zonder gegronde redenen en toestemming van de eigenaar de inhoud een persoonlijke mailbox lezen. Wel kan indien er gegronde redenen zijn en alleen met toestemming van het Bevoegd Gezag een mailbox van een gebruiker geopend worden door daarvoor aangewezen en geautoriseerde medewerkers.

3.c.3. Hoe gaan we met overtredingen om?

1. Een e-mailadres wordt (na overeenstemmend overleg met de directie) onmiddellijk uit de bestandenlijst verwijderd, wanneer wordt vastgesteld dat er:
    a. onwettige activiteiten mee gepleegd worden;
    b. porno, geweld en/of discriminerende taal mee ontvangen en/of verspreid en/of doorgegeven wordt;
    c. gepest wordt;
2. De betrokken gebruiker (c.q. ouders van) wordt daarvan in kennis gesteld door de directie. Tevens wordt daarbij aangegeven waarom het e-mailadres wordt verwijderd.
3. De gebruiker van een e-mailadres krijgt bij minder ernstig misbruik een waarschuwing door middel van een gele kaart. Deze berisping wordt gegeven na overeenstemmend overleg met de groepsleerkracht van het kind. Indien niet tot een overeenstemming wordt gekomen, wordt de directie geraadpleegd en geeft die een doorslaggevend advies. Ouder(s)/voogd(en)/verzorger(s) worden daarvan onverwijld in kennis gesteld. Daarbij wordt aangegeven wat de reden van deze berisping is.
4. Betreft het een personeelslid of een persoon die vanwege zijn/haar activiteiten op school ook een e-mailadres heeft gekregen, wordt advies gevraagd aan de directeur. Afhankelijk van de uitkomst van dat overleg, wordt actie ondernomen. In principe is de directeur met deze taak belast.
5. De systeembeheerder (hier wordt de e-mailbeheerder op schoolniveau bedoeld) draagt er zorg voor dat, zodra hij/zij melding krijgt van mogelijk misbruik dit gecontroleerd wordt en vervolgens onverwijld meldt aan de groepsleerkracht, indien het een leerling betreft en aan de directie wanneer het een volwassene betreft.
   De e-mailbeheerder draagt er zorg voor dat wanneer het e-mailadres verwijderd moet worden, dit onverwijld gebeurt.
6. De school draagt er zorg voor dat de leerlingen op school tekst en uitleg krijgen over het gebruik en misbruik van het e-mailadres. Volwassenen krijgen dergelijk instructies in ieder geval ook schriftelijk.

3.d. Privacy

3.d.1. Algemeen:

Onze website(s) en in gebruik zijnde sociale media platformen zijn het venster naar de wereld. We willen graag daar zo optimaal mogelijk gebruik van maken.
Helaas is het zo dat de kans bestaat dat niet iedere bezoeker oprecht is in zijn bezoek. Ter bescherming van onze leerlingen en door wetgeving hebben we een aantal afspraken vastgelegd.

3.d.2. Afspraken:

Op de website van de school, My Learning of alle andere in gebruik zijnde sociale media platformen worden foto's van activiteiten geplaatst die op school of namens school hebben plaatsgehad. Hierbij wordt door de webmaster de volgende regels in acht genomen:

- Foto's en filmpjes waarop leerlingen herkenbaar staan, mogen uitsluitend gepubliceerd worden als de ouders/verzorgers van de desbetreffende leerlingen hiermee akkoord zijn. Scholen vragen jaarlijks voor verschillende door de school gebruikte media hiervoor toestemming aan de ouders/verzorgers. Dit geldt ook voor het verspreiden van privacygevoelige gegevens zoals die staan op adres- en bellijsten
- Er wordt nooit een foto geplaatst waar een leerling alleen en frontaal op staat (portretfoto).
- Er worden foto's geplaatst waar kinderen "en profile" opstaan of in groepjes, mits er toestemming is.
- Suggestieve foto's worden nooit geplaatst.
- Foto's van gymmende kleuters in de speelzaal worden niet geplaatst. Foto's van kinderen in zwemkleding worden niet geplaatst. Foto's van andere sportende kinderen worden met terughoudendheid geplaatst.

Om persoonsgegevens te mogen verwerken kent de Algemene Verordening Gegevensbescherming een aantal uitgangspunten. Deze voorwaarden gelden voor elke school/organisatie en zijn samengevat tot 5 vuistregels. Aan deze vuistregels houdt de school zich:
1. Doel en doelbinding: Persoonsgegevens worden alleen gebruikt voor uitdrukkelijk voorafgaand aan de verwerking omschreven en gerechtvaardigde doeleinden. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. 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.
3. Dataminimalisatie: de persoonsgegevens die de school verwerkt, moeten redelijkerwijs nodig zijn om het doel te bereiken. De gegevens moeten in verhouding staan tot het doel. Dit betekent ook dat data niet langer wordt bewaard dan wat de wetgeving voorschrijft.
4. Transparantie: De betrokkene (medewerker, leerling en/of zijn ouders) is vooraf in begrijpelijke taal geïnformeerd over wat er precies aan informatie wordt verwerkt en wat het doel daarvan is. Verder hebben deze betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Daarnaast kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.
5. Data-integriteit: Maatregelen om te waarborgen dat te verwerken Persoonsgegevens juist en actueel zijn. Bij vermelding van persoonlijke gegevens van hen die bij de school zijn betrokken, zal nooit meer worden gepubliceerd dan vrij verkrijgbare informatie (informatie die publiekelijk te vinden is via diverse media).

3.d.3. Hoe gaan we met overtredingen om?

Bij publicatie van informatie, waar een betrokkene bezwaar tegen maakt, zal de webmaster deze informatie op verzoek verwijderen.

3.d.4. Wie grijpt in?

Bij overtredingen op My Learning in de klasgroepen zal de beheerder de informatie van de site verwijderen en eventueel de rechten van publicatie aanpassen.

De directeur beslist over de gevolgen van de overtreding.

3.e. Internetcontent filtering

3.e.1. Algemeen

Iedere school heeft de mogelijkheid om internetsites te filteren. Men kan kiezen voor content filtering. Dit kan middels “whitelisting” (Niets mag, behalve…) of “Blacklisting” (Alles mag, behalve…). Het gaat om software die “onzichtbaar” op de achtergrond zijn werk doet. Zodra de gebruiker probeert toegang te krijgen tot een website met schadelijke inhoud wordt het filter “zichtbaar” en blokkeert de toegang tot die site. De plaats waar de scheidslijn wordt getrokken tussen wat wel en niet schadelijk is, kan bij veel filters worden ingesteld.

Filtering op NBS De Hoogakker

Op NBS De Hoogakker wordt geen gebruik gemaakt van filtering van websites. Het team van NBS De Hoogakker is van mening dat leerlingen een attitude moet worden aangeleerd om bewust met het medium Internet en sociale media om te gaan. We hangen dan ook de filosofie van begeleid confronteren aan.

3.e.2. Afspraken:

Aan het begin van ieder schooljaar bespreken de kinderen met de leerkrachten de regels omtrent het gebruik van Internet in de klas en op school. Er wordt een door de kinderen opgesteld protocol gemaakt dat de kinderen ondertekenen (Internetcontract). De leerkracht zal de gemaakte afspraken herhalen met de groep.

3.e.3. Hoe gaan we met overtredingen om?

Leerkrachten die geen internetprotocol in de klas hebben zullen dit moeten maken. Indien het wel aanwezig is, maar er niet naar gehandeld wordt, zal dit wel moeten gebeuren.

3.e.4. Wie grijpt in?

De ICT coördinator kan de betreffende leerkracht helpen bij het maken van een Internetprotocol. Bij (voortdurend) uitblijven van een Internetprotocol zal de directeur dit item bespreken tijdens een (functionerings-) gesprek.

3.f. Overige Communicatiemiddelen: Chatten/Profielsites/Mobiele telefonie

3.f.1. Algemeen:

In de huidige samenleving is chatten, het maken en onderhouden van profielsites en mobiele telefonie gemeengoed. Hoewel aan deze media ook uitstekende eigenschappen zitten, is het gebruik hiervan binnen de school niet altijd wenselijk.

3.f.2. Afspraken:

Het is in de klas niet toegestaan gebruik te maken van chatdiensten.
Leerkrachten chatten niet met leerlingen. Ook niet na schooltijd.
Het is niet toegestaan om profielsites op school te onderhouden zoals onder andere Facebook, Instagram en Linkedin
Leerkrachten abonneren zich niet op profielsites van leerlingen. Ook ingaan op vriendenuitnodigingen van leerlingen via gameconsoles zoals PlayStation 4 en Xbox is niet toegestaan of via gameplatforms als Twitch of Steam.
Het is niet toegestaan om deel uit te maken van een leerling WhatsApp groep of gehele WhatsApp klasgroep. Contact met klassenouder via WhatsApp mag wel, zolang de wet op privacy niet wordt overtreden. Foto's delen met je klassenouder via WhatsApp is dus niet toegestaan.

Mobiele telefoons zijn privé in gebruik. Toch kunnen er onwenselijke situaties ontstaan vanwege mobiele telefoons. Het is daarom goed als school de mogelijkheden en gevaren van mobiele telefoons goed te kennen. Een aantal regels en afspraken is daarom wenselijk.

Kinderen:

- De mobiele telefoon mag van huis meegenomen worden naar school.
- Tijdens de middagpauze mogen ze worden gebruikt voor internettoepassingen.
- Op andere momenten mag de mobiele telefoon slechts met toestemming van de leerkracht worden gebuikt.
- De leerlingen mogen met hun mobiele telefoon gebruik maken van het gastennetwerk op de WIFI van de SNB.
- Om dringende redenen mag de mobiele telefoon worden gebruikt om te bellen na overleg met de leerkracht.
- De mobiele telefoon mag **niet** worden gebruikt voor het maken van film-, foto- en/of geluidsopnames tijdens schoolactiviteiten. Hieronder valt:
  - activiteiten in de klas, gang, toilet, in de hal of op het plein van de school
  - het omkleden in de kleedkamer of elders en tijdens de gym- en sportactiviteiten
  - buitenschoolse activiteiten e.d. In een aantal van dit soort situaties (b.v. tijdens excursie, kamp) is het wel toegestaan om foto's te maken. De leerkracht geeft dan toestemming en ziet er tijdens of na de fotosessie op toe dat er geen afbeeldingen gemaakt zijn die ingaan tegen goede smaak of integriteit van personen.
- Het meenemen van eigen devices naar school, gebeurt (nog) niet op verzoek van school en op eigen verantwoording.

Leerkrachten:

- Het is de leerkrachten niet toegestaan tijdens schooltijd hun mobiele telefoon aan te hebben staan voor privégebruik.
- Leerkrachten die om een geldende reden privé toch bereikbaar willen zijn, stellen de locatieleider hiervan op de hoogte.
- Tijdens vergaderingen en onder lestijden kan de leerkracht gebruik maken van zijn mobiele telefoon onder de voorwaarde dat hij werk gerelateerde apps en functies gebruikt. Hieronder kan bijvoorbeeld worden verstaan: Parnassys app, My Learning app of Calenders app tijdens vergadertijd of tijdens lestijden kan gebruik worden gemaakt van Kahoot, Menti of TooNoisy Bij het maken van film-, foto- en/of geluidsopnames moet de leerkracht zich houden aan de Algemene Verordening Gegevensbescherming.
- Leerkrachten hebben geen niet-functionele contacten met (oud-) leerlingen of ouders via computer en/of mobiele telefoon.

3.f.3. Hoe gaan we met overtredingen om?

- Bij gebruik van een mobiele telefoon zonder toestemming, neemt de leerkracht het toestel in beslag. Na schooltijd kan het kind het toestel weer terug vragen.
- Leerkrachten worden aangesproken op het privégebruik van een mobiele telefoon onder werktijd.

3.f.4. Wie grijpt in?

- De gebruiker van een mobiele telefoon krijgt bij minder ernstig misbruik een waarschuwing door middel van een gele kaart door de directeur. Deze berisping wordt gegeven na overeenstemmend overleg met de groepsleerkracht van het kind. Indien niet tot een overeenstemming wordt gekomen, wordt de directie geraadpleegd en geeft die een doorslaggevend advies. Ouder(s)/voogd(en)/verzorger(s) worden daarvan onverwijld in kennis gesteld. Daarbij wordt aangegeven wat de reden van deze berisping is.
- De leerkracht waarschuwt de leerling bij overtreding van de afspraak.
- Bij een volgende overtreding volgt een waarschuwing van de locatieleider.
- Bij de derde overtreding wordt de mobiele telefoon door de locatieleider in beslag genomen en worden de ouders geïnformeerd.
  De telefoon wordt aan de ouders teruggegeven.
- Indien een leerkracht de afspraken negeert, wordt hij/zij hierop aangesproken door de locatieleider.
- Bij herhaalde overtreding stelt de locatieleider de directeur hiervan op de hoogte. Deze laatste zal gepaste maatregelen treffen.