Protocol Mediagebruik:

Inleiding

Zowel met betrekking tot het gebruik van tv / video / internet als m.b.t. het gebruik van social media staan wij op het standpunt dat ongewenste uitingen zoveel mogelijk moeten worden voorkomen. Hoewel het omgaan met dergelijke media zeker ook als leerpunt gezien wordt, leert de praktijk van het dagelijks leven ons dat het beter is om te voorkomen dan om te genezen. TriVia vertrouwt erop dat zijn medewerkers, leerlingen en alle andere bij TriVia betrokkenen, verantwoord om zullen gaan met de vele mogelijkheden die de diverse media ons bieden. TriVia heeft dit protocol opgesteld om een ieder die bij TriVia en / of één van onze scholen werkzaam en / of betrokken is of zich daarbij betrokken voelt, daarvoor richtlijnen te geven.

Uitgangspunten bij tv-gebruik, videogebruik, omgang met social media en internetten

- Onze scholen bevorderen het verantwoordelijkheidsgevoel bij leerlingen door de toegang tot internet en videobeelden te begeleiden.
- Onze scholen stellen kinderen niet bewust bloot aan beelden van geweld, seks en racisme, die geen opvoedkundige bedoeling hebben.
- Bij het vertonen van dvd's wordt met de leeftijdscategorie rekening gehouden, films voor 12 jaar en ouder worden **nooit** vertoond!
- Onze scholen zien het als opvoedkundige taak om kinderen ervan bewust te maken waarom bepaalde uitingen niet kunnen.
- Onze scholen proberen te voorkomen dat ongewenste uitingen de scholen binnenkomen.
- Leerlingen mogen niet onbeperkt en onbelemmerd internetten; personeel van de school kijkt als het ware "over de schouder mee".
- Onze scholen proberen hun leerlingen bij te brengen welke zoekopdrachten wel en welke niet relevant zijn bij het zoeken naar informatie op internet.

- Chatten door leerlingen wordt niet toegestaan en m.b.v. YourSafetyNet School+ onmogelijk gemaakt op het computernetwerk.
    - Chatsessies worden door YourSafetyNet School+ gelogd en bij de geadresseerde(n) verschijnt een unieke waarschuwingsboodschap, om kwaadwillenden af te schrikken.
    - Ook het IP-adres van de geadresseerde(n) wordt door YourSafetyNet School+ gelogd, om bij misbruik de dader(s) op te kunnen sporen.
- Het leggen van contacten via "social media" door leerlingen is niet toegestaan en wordt m.b.v. YourSafetyNet School onmogelijk gemaakt op het netwerk
- Het bewust zoeken van ongewenste uitingen en het gebruik van schuttingtaal door leerlingen wordt als storend opgevat en heeft dus consequenties voor de leerling.
- Het beleid wordt ouders/verzorgers meegedeeld in de schoolgids en op de website van de school.
- Op alle netwerkcomputers wordt gebruik gemaakt van Internet Explorer met een geïntegreerde pop-upblokkering, waardoor heel veel popup-vensters (met veelal ongewenste reclame) geblokkeerd worden. De systeembeheerder heeft de policies op het netwerk zodanig ingesteld, dat deze pop-upblokkering niet uitgeschakeld kan worden.
- Het SmartScreen-filter (ook onderdeel van Internet Explorer) is ook op alle netwerkcomputers ingeschakeld en kan door de ingestelde policies niet door gebruikers uitgeschakeld worden. *(Het SmartScreen-filter is een functie van Internet Explorer waarmee phishingwebsites worden opgespoord. Het SmartScreen-filter voorkomt tevens dat schadelijke software of malware (dit zijn programma's die virussen bevatten of illegaal, frauduleus of schadelijk gedrag vertonen) geïnstalleerd kan worden)*
- De InPrivate-navigatie (onderdeel van Internet Explorer) is op alle netwerkcomputers uitgeschakeld en kan door de ingestelde policies niet door gebruikers ingeschakeld worden. *(Met InPrivate-navigatie kan er op internet gewerkt worden zonder een spoor achter te laten in Internet Explorer. Met InPrivate-navigatie wordt voorkomen dat anderen kunnen zien welke websites een gebruiker heeft bezocht. Door deze optie uit te schakelen wordt het anoniem internetgebruik voorkomen)*
- De systeembeheerder heeft de policies op het netwerk zodanig ingesteld, dat de gebruikers hun internethistorie niet kunnen wissen. M.b.v. YourSafetyNet School+ wordt de internethistorie van alle gebruikers centraal op de server opgeslagen en voor bepaalde tijd bewaard.
- Door sociale controle wordt ook veel ongewenst gedrag voorkomen.

Afspraken met de kinderen

- Geef nooit persoonlijke informatie door op Internet, zoals namen, adressen, leeftijd en telefoonnummers, zonder toestemming van de leerkracht.
- Vertel het je leerkracht meteen als je informatie tegenkomt waardoor je je niet prettig voelt of waarvan je weet dat dat niet hoort. Houd je je aan de afspraken, dan is het niet jouw schuld wanneer je zulke informatie tegenkomt.
    - M.b.v. de zgn. alarmknop van YourSafetyNet School+ (rechts onderin de taakbalk) kan een printscreen van de ongewenste website e.d. gemaakt worden.
    - Deze printscreen wordt centraal op de server opgeslagen en kan door de systeembeheerder uitgelezen worden.
- Leg nooit verdere contacten met iemand zonder toestemming van je leerkracht.
- E-mail alleen naar bekenden.
- Verstuur bij e-mail berichten nooit foto's van jezelf of van anderen zonder toestemming van je leerkracht.

- Beantwoord nooit e-mail waarbij je je niet prettig voelt of waar dingen in staan waarvan je weet dat dat niet hoort. Het is niet jouw schuld dat je zulke berichten krijgt.
- Verstuur ook zelf dergelijke mailtjes niet. Meestal is te achterhalen wie een mailtje heeft verstuurd.
- Iedereen houdt zich aan de afspraken zoals die door de kinderen bij het behalen van hun diploma Veilig Internet geleerd zijn
- Digipesten in welke vorm dan ook, wordt niet toegestaan.
- Spreek van tevoren met je leerkracht af wat je op internet wilt gaan doen.
- Gebruik internet alleen voor educatieve doeleinden
- Buiten de schooltijden om mogen de kinderen alleen gebruik maken van de computers *met toestemming van de leerkracht*.
- Steeds meer leerlingen bes*chikken over een mobiele telefoon.* Deze telefoons dienen onder schooltijd uit te staan. *(als leerkrachten mag je ze dus niet horen of zien)* Met mobiele telefoons mogen geen beelden op school gemaakt worden.

Afspraken met de medewerkers

- Het computernetwerk in het schoolgebouw is voor alle collega's beschikbaar op 6 dagen van de week. Op zondag is dit netwerk niet beschikbaar.
- Zodra het netwerk van een school via internet benaderd kan worden, zal dit netwerk alle dagen van de week voor iedereen toegankelijk zijn.
    - Dagelijks wordt er tussen 24.00 uur en 07.00 uur een back-up van het netwerk gemaakt. Indien er door personeel tijdens deze uren op het netwerk gewerkt wordt, is het mogelijk dat er van dit werk geen back-up gemaakt wordt. Dat zal dan de volgende nacht gebeuren.
    - Indien een personeelslid, vanuit zijn / haar eigen verantwoordelijkheid, besluit om op zondag gebruik te maken van het netwerk, is het voor hem / haar **niet** toegestaan om mail te versturen naar ouders / verzorgers / kinderen.
- De kinderen mogen buiten de schooltijden om *alleen* met jullie toestemming gebruik maken van de computer.
- Internet, tv en video worden gebruikt voor opbouwende educatieve doeleinden.
- Mocht een collega software willen downloaden en installeren voor schoolgebruik, dan gebeurt dat alleen door de systeembeheerder. Het computernetwerk is zodanig beveiligd, dat gebruikers geen software kunnen installeren.
- Er worden geen sites bekeken die niet aan onze fatsoensnormen voldoen.
- Er wordt aan de kinderen uitgelegd waarom zij bepaalde sites wel of niet mogen bekijken.
- De leerkracht draagt zorg voor een omgeving waarin kinderen open kunnen vertellen wanneer zij op een ongewenste, onbedoelde site komen. Het is meestal immers niet hun schuld.
- Regels en wetten met betrekking tot copyright worden zoveel mogelijk gerespecteerd (kopiëren van cd's, dvd's etc. voor gebruik binnen school zijn toegestaan, evenals voor eigen gebruik, maar voor derden buiten school en voor eventuele verkoopdoeleinden niet!).
- Informatie die terug te voeren is op leerlingen mag niet op het openbare deel van het internet terechtkomen.
- Volledige namen in combinatie met foto's van kinderen worden niet op het internet gepubliceerd.
- Voor het publiceren van individuele foto's wordt eerst toestemming aan de ouders / verzorgers gevraagd.
- Er worden nooit foto's van kinderen in weinig verhullende kleding gepubliceerd.
- Voor e-mail geldt ook het briefgeheim, maar op grond van hun pedagogische verantwoordelijkheid mogen de leerkrachten e-mail van leerlingen bekijken.
- Digipesten in welke vorm dan ook wordt krachtig tegengegaan

    - In voorkomende gevallen wordt hier speciale aandacht aan besteed, bijv. via een lessenserie van Hyves.
- Contacten door leerkrachten met leerlingen op alle mogelijke “social media” zijn niet toegestaan, met uitzondering van het navolgende punt:
- Het is leerkrachten en directies wel toegestaan om school- / groepsgerelateerde mededelingen via Twitter onder een groep leerlingen / onder groepen leerlingen en/of onder hun ouders te verspreiden, onder voorwaarde dat dit alleen toegestaan is in groep 8, dat we hier een jaar mee experimenteren en daarna (in december 2013) evalueren of deze werkwijze bij TriVia past.
- De leerkrachten zorgen ervoor dat de kinderen bekend worden gemaakt met de hierboven genoemde “regels voor de kinderen”.
- Tijdens de lessen staan de mobiele telefoons uit.
- Voor het gebruiken van alle EIC–middelen zijn per 1-8-2010 in een gelijknamig beleidsstuk afspraken gemaakt omtrent het handelen van ons personeel (op het bureaublad van het personeel wordt hier ook melding van gemaakt).
- TriVia is voorstander van heldere communicatie met ouders. Het gebruik van social media is, naast de website een toegevoegde waarde.
- Medewerkers van TriVia kunnen kennis en andere waardevolle informatie delen via social media.
- Bij onderwijs onderwerpen maken medewerkers duidelijk of zij op persoonlijke titel of namens “hun” school publiceren.
- Medewerkers van onze scholen publiceren geen vertrouwelijke informatie op social media.
- Social media is een goed medium om te communiceren, het is echter niet de bedoeling om met ouders of leerlingen een discussie te voeren.
- Schoolbestuurders, schoolleiders en leidinggevenden zijn altijd vertegenwoordiger van de school – ook als zij een privé-mening verkondigen. Bij twijfel niet publiceren.
- Medewerkers van onze scholen zijn persoonlijk verantwoordelijk voor wat zij publiceren.
- Medewerkers van onze scholen weten dat publicaties op social media altijd vindbaar zijn.
- Bij twijfel over een publicatie of over de raakvlakken met “hun” school zoeken medewerkers contact hun leidinggevende.

Afspraken in het belang van de leerlingen:

- Na de eerste constatering van ongewenst gebruik wordt de betreffende leerling door de groepsleerkracht aangesproken op zijn / haar ongewenste gedrag.
    - De groepsleerkracht bespreekt het voorval met de schooldirectie. Hierna wordt dit voorval + de bij herhaling van een dergelijk voorval te nemen maatregelen, met de betreffende ouders door de groepsleerkracht besproken.
- Na de tweede constatering van ongewenst gebruik wordt de betreffende leerling door de schooldirectie aangesproken op zijn / haar ongewenste gedrag en wordt hem / haar medegedeeld dat hij / zij gedurende 3 maanden alleen onder direct toezicht van zijn / haar leerkracht gebruik zal mogen maken van ons computernetwerk.
    - De groepsleerkracht bespreekt het voorval met de schooldirecteur. De schooldirecteur bespreekt dit voorval hierna met de betreffende ouders en legt de te nemen maatregel uit.
- Na een eventuele derde constatering van ongewenst gebruik wordt de betreffende leerling door de schooldirectie opnieuw aangesproken op zijn / haar ongewenste gedrag en wordt hem / haar medegedeeld dat hij / zij tot nader order = minimaal 6 maanden, op geen enkele wijze gebruik zal mogen maken van ons computernetwerk. (dit wordt z.s.m. doorgegeven aan de

systeembeheerder, zodat de systeembeheerder de toegang tot het computernetwerk voor de desbetreffende gebruiker kan blokkeren).
    - De groepsleerkracht bespreekt het voorval met de schooldirecteur. De schooldirecteur bespreekt dit voorval hierna met de betreffende ouders en legt de te nemen maatregelen uit.

Afspraken in het belang van de medewerkers:

- Minstens een keer per jaar wordt m.b.v. YourSafetyNet School+ gedurende één maand een logfile bijgehouden van alle elektronische informatie- en communicatiemiddelen-verkeer. Deze controle vindt plaats door een externe systeembeheerder.
- De geanonimiseerde rapportage van deze logfile wordt door de externe systeembeheerder verstrekt aan de directeur - bestuurder en aan de schooldirecteur.
    - Deze rapportage wordt jaarlijks besproken tijdens het locatieoverleg.
    - De directeur - bestuurder kan naar aanleiding van deze rapportage vragen om een gepersonaliseerde rapportage.
- Indien een personeelslid of een groep personeelsleden ervan wordt verdacht de regels te overtreden, kan gedurende een vastgestelde (korte) periode gerichte controle plaatsvinden.
- De directeur - bestuurder geeft, na hierover ingelicht te zijn door de schooldirecteur, in voorkomende gevallen aan de externe systeembeheerder de opdracht om de elektronische informatie- en communicatiemiddelenacties van de betrokkene(n) na te gaan.
- De externe systeembeheerder brengt hiervan schriftelijk verslag uit aan de directeur - bestuurder . Deze bespreekt dit verslag met de betreffende schooldirecteur.
- In geval van misbruik door de schooldirecteur wordt hierover door de extern systeembeheerder verslag uitgebracht aan de directeur - bestuurder .
- Het computernetwerk op de school zelf is voor alle directieleden beschikbaar op alle dagen van de week.
- Zodra een netwerk via internet benaderd kan worden zal dit netwerk alle dagen van de week voor al ons personeel toegankelijk zijn.

Afspraken in het belang van de directie

- In geval van misbruik door de schooldirecteur wordt hierover door de extern systeembeheerder overleg gevoerd met de directeur - bestuurder .
- Aansluitend hierop vindt er een gesprek plaatst tussen de directeur - bestuurder en de schooldirecteur
- Indien de adjunct-schooldirecteur misbruik maakt spreekt de schooldirecteur hem / haar hier op aan.
- Indien de directeur - bestuurder misbruik maakt, dan wordt dit door de extern systeembeheerder gemeld bij de voorzitter van het toezichthoudend schoolbestuur.
    - Deze treedt hierover in overleg met de andere leden van het schoolbestuur.
    - Deze spreken in gezamenlijk overleg een te volgen traject af.
- Ingeval van ongewenst gebruik door leerkrachten spreekt de schooldirecteur de betreffende collega op zijn / haar ongewenste gedrag aan.

Vastgesteld AB 09-11-2011 / GMR 28-11-2011/ definitief vastgesteld AB 14-12-2011

Opnieuw vastgesteld in AB 14-11-2012/ GMR 22-11-2012 / definitief vastgesteld AB 12-12-2012