Protocol sociale media & internetfaciliteiten

Inhoudsopgave

Inleiding

Sociale media zoals Whatsapp, Telegram, Twitter, LinkedIn, Facebook, SnapChat, TikTok, Instagram, blogs en YouTube zijn niet meer uit ons leven weg te denken. Ze maken communicatie een stuk sneller en makkelijker en wij maken er allemaal dankbaar gebruik van. Via de sociale media kun je ook laten zien dat je trots bent op je school en je berichten kunnen een bijdrage leveren aan een positief imago van de school.

Maar bij verkeerd gebruik kunnen er ook vervelende gevolgen optreden. Een bericht op sociale media is snel geplaatst en je kunt er veel mensen in een korte tijd mee bereiken. Daarmee kan dus ook 'de impact' van een bericht groot zijn en onvoorziene/onbedoelde gevolgen teweegbrengen. Het is daarom van belang te beseffen dat je met berichten op sociale media (onbewust) ook de goede naam van de school en betrokkenen kunt schaden. Dit geldt voor iedereen die met de school verbonden is zoals leerlingen, ouders, verzorgers, medewerkers en vrijwilligers. Om deze reden vragen wij om bewust met sociale media om te gaan. Essentieel is dat, net als in communicatie buiten de digitale wereld, de gebruikers van sociale media de reguliere fatsoensnormen respecteren en de nieuwe/digitale mogelijkheden met een positieve instelling benaderen. Zie hiervoor ook de binnen Stichting Limburgs Voortgezet Onderwijs (hierna: LVO) geldende beleidsvisie Horizon 2025 en de huisregels van de scholen.

Als medewerker ben je ambassadeur van *[LVO/naam school]*. Je wordt als persoon en in jouw (online) gedrag altijd gezien als onderdeel van de school, óók in je vrije tijd (zowel in positieve als in negatieve zin): wees je daar bewust van. Alle medewerkers hebben een voorbeeldfunctie en we vragen je daar in je gedrag bewust van te zijn.

Dit protocol bevat ook regels omtrent het gebruik van internetfaciliteiten van LVO. Onder internetfaciliteiten wordt o.a. verstaan:

- door LVO of school beschikbaar gestelde apparatuur zoals laptops en telefoons,
- internet en intranet,
- Microsoft Office 365 softwaretoepassingen (zoals o.a. Outlook, Word, OneNote),
- andere geïnstalleerde software applicaties (zoals o.a. Microsoft Teams, Microsoft OneDrive, Microsoft SharePoint, LAS en ELO)

De internetfaciliteiten zijn bestemd voor het uitvoeren van de door [*LVO/naam school]* aan de gebruiker (medewerker, leerling, andere aan de school verbonden personen) opgedragen taken. Het privégebruik van de internetfaciliteiten is slechts in beperkte mate toegestaan en binnen de maatschappelijk toelaatbare grenzen. Wij gaan ervan uit dat elke gebruiker weet dat er geen plaats is voor incorrecte, onfatsoenlijke, onzedelijke, misleidende of anderszins onrechtmatige handelingen, uitlatingen en discussies. Het protocol bevat afspraken over de wijze waarop *[LVO/naam school]* omgaat met het registreren, verzamelen en monitoren van tot een persoon herleidbare data in verband met gebruik van de internetfaciliteiten. Het doel is om een goed evenwicht te vinden tussen een verantwoord gebruik van de internetfaciliteiten enerzijds, waarbij de belangen van de LVO en de school, de medewerkers en leerlingen centraal staan, en de bescherming van de privacy van leerlingen en medewerkers anderzijds.

Dit protocol is bestemd voor leerlingen, ouders/verzorgers, medewerkers (inclusief ingehuurd personeel, stagiaires en vrijwilligers), en anderen die zijn verbonden aan *[LVO/naam school]*. Daar waar de regels en richtlijnen specifiek voor één van de hiervoor genoemde groepen gelden, wordt dit uitdrukkelijk vermeld. Het protocol geldt LVO-breed en geldt dus voor alle onder LVO vallende scholen en de ondersteunende diensten.

[LVO/naam school] vertrouwt erop dat haar leerlingen, ouders/verzorgers, medewerkers en andere betrokkenen verantwoord om gaan met het gebruik van sociale media en de internetfaciliteiten en heeft dit protocol opgesteld om eenieder die bij *[LVO/naam school]* betrokken is of zich daarbij betrokken voelt daarvoor richtlijnen te geven.

Het college van bestuur
van Stichting Limburgs Voortgezet Onderwijs

22 december 2021

Deel I: Sociale media

Sociale media is een verzamelnaam voor alle internettoepassingen die het mogelijk maken om informatie met elkaar te delen op een eenvoudige en vaak leuke manier. Het gaat hierbij niet alleen om informatie in de vorm van tekst (nieuws, artikelen), maar ook om geluid (podcasts, muziek) en beeld (fotografie, video) die worden gedeeld via sociale media (zoals Instagram, TikTok, Facebook, Twitter, YouTube, SnapChat, WhatsApp, Telegram enz.). De essentie van sociale media is dat iemand er informatie deelt over zichzelf, over anderen of over een bepaald onderwerp.

A. Uitgangspunten

1. *[LVO/naam school]* onderkent het belang van sociale media en zet berichtgeving op sociale media in met het doel om relevante informatie te verspreiden over de (activiteiten van de) school of organisatie.
2. Het protocol draagt bij aan een goed en veilig school- en onderwijsklimaat.
3. Het protocol bevordert dat de school leerlingen, ouders/verzorger, medewerkers en vrijwilligers op sociale media communiceren in het verlengde van de missie en visie van *[LVO/naam school]* en de reguliere fatsoensnormen. In de regel betekent dit dat we respect voor de school en elkaar hebben en iedereen in zijn/haar waarde laten.
4. De gebruikers van sociale media dienen rekening te houden met de goede naam van (*LVO/naam school)* en van eenieder die daarbij betrokken is. Medewerkers hebben hier een voorbeeldfunctie.
5. Het protocol dient (*LVO/ naam* school), haar leerlingen, ouders/verzorger, medewerkers en vrijwilligers tegen zichzelf en anderen te beschermen voor de mogelijke negatieve gevolgen van sociale media.
6. *(LVO/naam school)* verwacht van haar leerlingen en medewerkers dat zij zich conformeren aan dit protocol. Bij niet in lijn handelen met dit protocol, zal hierover het gesprek met de betreffende persoon worden aangegaan.
7. Indien de internetfaciliteiten van LVO worden gebruikt voor sociale media, dan zijn de in deel 2 van dit protocol geldende regels en richtlijnen met betrekking tot het gebruik van internetfaciliteiten tevens van toepassing.

B. Doelgroep en reikwijdte

1. Deze richtlijnen zijn bedoeld voor alle betrokkenen die deel uitmaken van de LVO/schoolgemeenschap, dat wil zeggen leerlingen, ouders/verzorger, medewerkers, vrijwilligers en mensen die op een andere manier verbonden zijn aan *[LVO/naam school].*
2. De richtlijnen in dit protocol hebben alleen betrekking op LVO- of schoolgerelateerde berichten of wanneer er een overlap is tussen school, werk en privé.
3. De richtlijnen hebben verder niet alleen betrekking op het plaatsen van berichten maar ook op het delen daarvan op sociale media.

C. Sociale media in de school

Voor alle gebruikers (medewerkers, leerlingen, ouders/verzorgers en vrijwilligers)

1. Het is betrokkenen toegestaan om kennis en informatie te delen, mits het geen persoonsgegevens betreft en andere betrokkenen niet schaadt.
2. Het is betrokkenen niet toegestaan om tijdens de lessen actief te zijn op sociale media dan wel beeld- en/of geluidsopnamen te maken en/of deze te verspreiden, tenzij door de schoolleiding respectievelijk de docent hiervoor vooraf toestemming is gegeven.
3. De betrokkene is in alle gevallen zelf verantwoordelijk voor de inhoud die hij/zij publiceert op sociale media. Het is de betrokkene niet toegestaan om anonieme berichten te plaatsen of te verspreiden die anderen of de school schaden.

4. Elke betrokkene dient zich ervan bewust te zijn dat de gepubliceerde teksten en uitlatingen voor onbepaalde tijd openbaar zullen zijn, ook na verwijdering van het bericht.
5. *[LVO/naam school]* vraagt aantoonbaar schriftelijk toestemming aan ouders of leerlingen ouder dan 16 jaar en medewerkers om foto-, film- en geluidsopnamen van aan school gerelateerde situaties, waarop zij herkenbaar zijn afgebeeld, op sociale media van *[LVO/naam school]* te zetten.
6. Betrokkenen nemen de reguliere fatsoensnormen jegens elkaar en derden in acht. Indien handelingen worden verricht die in strijd zijn met de reguliere fatsoensnormen en/of (mogelijk) een strafbaar karakter hebben (bijvoorbeeld: het hacken van een account, radicalisering, sexting, pesten, stalken, bedreigen, het verspreiden van memes of anderszins beschadigende inhoud) dan neemt *[LVO/naam school]* passende maatregelen.[1]
7. Indien een betrokkene kennis heeft van ontoelaatbare en/of grensoverschrijdende communicatie in woord, beeld en/of geluid dan dient hij/zij dat te melden bij de schoolleiding van [*naam school*] of bij het college van bestuur van LVO.

Voor medewerkers

1. Medewerkers hebben een bijzondere verantwoordelijkheid bij het gebruik van sociale media: *[LVO/naam school]* respecteert de vrijheid van meningsuiting van al haar medewerkers, maar privémeningen van medewerkers kunnen eenvoudig verward worden met de officiële standpunten van de school. Indien een medewerker deelneemt aan een discussie die (op enigerlei wijze) te maken heeft met *[LVO/naam school]* dient de medewerker te vermelden dat hij/zij medewerker is van *[LVO/naam school]* en duidelijk aan te geven dat dit een persoonlijke mening betreft en dat deze losstaat van eventuele officiële standpunten van *[LVO/naam school]*.
2. Het is de medewerker toegestaan om over schoolgerelateerde onderwerpen te publiceren op zijn eigen sociale media mits het geen vertrouwelijke of persoonsgebonden informatie over de school, haar medewerkers, leerlingen, ouders/verzorgers en andere betrokkenen betreft. De medewerkers zijn zich hierbij bewust dat zij ambassadeurs zijn van de school, het verspreiden van onjuiste of onware informatie dient te worden voorkomen en het in acht nemen van wettelijke – en fatsoensnormen bij een publicatie is essentieel en vanzelfsprekend. Bij een publicatie houdt de medewerker ook rekening met het belang van LVO of de school om de goede naam in stand te houden. Indien de medewerker van *[LVO/naam school]* een bericht publiceert waarin hij zijn persoonlijke mening verwoordt, dient dit bij het bericht te worden aangegeven.
3. Bij twijfel of een publicatie in strijd is met deze richtlijnen neemt de medewerker contact op met zijn/haar leidinggevende.
4. Medewerkers gaan niet in discussie met een leerling of ouder op sociale media.
5. Als online communicatie dreigt te ontsporen dient de medewerker direct contact op te nemen met zijn/haar leidinggevende om de te volgen strategie te bespreken.
6. Indien medewerkers dienen te communiceren met leerlingen, dan geschiedt dit via de door de [*LVO/naam school*] aangedragen kanalen (zoals het e-mailsysteem van LVO of het leerlinginformatiesysteem dat binnen [LVO/naam school] wordt gebruikt) en volgens de geldende fatsoensnormen. De medewerker dient zich er altijd bewust van te zijn dat hij/zij een professionele afstand tot de leerlingen heeft te bewaren. Dit betekent dat het contact tussen de medewerker en de leerling functioneel en schoolgerelateerd is. Het is de medewerker toegestaan om in bepaalde gevallen in bijvoorbeeld whatsapp in een groep met leerlingen aan te maken (bijvoorbeeld de mentor voor zijn mentorklas of een begeleider ingeval van excursies) om berichten aan die groep te kunnen sturen. Ook hier geldt dat de berichten functioneel en schoolgerelateerd dienen te zijn. .
7. Het is medewerkers niet toegestaan om via sociale media privéberichten te sturen aan leerlingen dan wel op privéberichten van leerlingen via sociale media te reageren.

[1] Zie ook deel III: gevolgen voor medewerkers en leerlingen.

Deel II: Gebruik internetfaciliteiten

A. Uitgangspunten

Dit deel van het protocol legt regels vast voor het gebruik van de internetfaciliteiten van LVO door leerlingen en medewerkers en de controle op de naleving hiervan. Het doel van dit deel van het protocol is om normen, regels en uitgangspunten vast te leggen ten aanzien van:

1. Systeem- en netwerkbeveiliging, inclusief beveiliging tegen schade en misbruik.
2. Het tegengaan van seksuele intimidatie, discriminatie en andere strafbare feiten.
3. De bescherming van privacygevoelige informatie, waaronder persoonsgegevens van leerlingen, medewerkers, ouders/verzorgers en vrijwilligers van *[LVO/naam school]* en daarmee het beschermen van de privacy en veiligheid van betrokkenen.
4. De bescherming van vertrouwelijke informatie van [*LVO/naam school*], haar leerlingen, ouders/verzorger, medewerkers, en vrijwilligers.
5. Het voorkomen en tegengaan van misbruik van de internetfaciliteiten.
6. De bescherming van de intellectuele eigendomsrechten van [*LVO/naam school*] en derden.
7. Het voorkomen van negatieve publiciteit.
8. Kosten- en capaciteitsbeheersing.

B. Algemene normen

Iedere leerling en medewerker houdt zich in ieder geval altijd aan de volgende zorgvuldigheidsnormen:

1. Ga zorgvuldig om met gegevens in verband met de privacy,
2. Zorg voor een goede fysieke en technische bescherming van bedrijfs- en of schoolmiddelen (beveiligingsmaatregelen),
3. Leef de beveiligingsmaatregelen na,
4. Meld diefstal of verlies van bedrijfs- en of schoolmiddelen onmiddellijk na constatering bij de leidinggevende of mentor en maak indien nodig melding van een mogelijk datalek via de procedure melden beveiligingsincidenten.
5. Voor medewerkers: Voorkom het lekken van interne en vertrouwelijke informatie.

C. Gebruik van internetfaciliteiten

Voor medewerkers

Computergebruik

Voor het uitoefenen van de werkzaamheden stelt *[LVO/naam school]* aan de medewerker computer- en netwerkfaciliteiten ter beschikking. Het gebruik van deze middelen is verbonden aan deze werkzaamheden en gaat uit van de volgende uitgangspunten:

1. Zorg dat privacygevoelige gegevens niet toegankelijk zijn voor onbevoegden.
2. Weet welke gegevens er mogen worden gebruikt en welke ICT-voorzieningen kunnen worden ingezet bij het verrichten van de verschillende schoolwerkzaamheden.
3. Sla (persoons)gegevens alleen op de daarvoor aangewezen systemen op.
4. Versleutel alle gegevens met betrekking tot *[LVO/naam school]*, indien deze gegevens, om welke redenen dan ook, elders opgeslagen worden.
5. Deel wachtwoorden nooit, ook niet incidenteel. Wachtwoorden zijn persoonlijk.
6. Sluit na gebruik de computer af of log uit.
7. Meld storingen van beheerde werkplekken (computer of laptop) bij de afdeling ICT.

Het is niet toegestaan bestanden met pornografische, racistische, discriminerende, gewelddadige of anderszins onacceptabele, dan wel niet voor het onderwijs aan [*LVO/naam school*] bestemde inhoud te downloaden, op het netwerk te plaatsen, in bezit te hebben, te delen of van deze bestanden gebruik te maken. Dit geldt ook voor het openen van deze bestanden via externe drives.*Werkplek*

Voorkom dat anderen (onbedoeld) toegang kunnen krijgen tot bedrijfsmiddelen en gegevens waartoe zij geen rechten hebben. Als aanvullende regels gelden:

1. Vergrendel de computer bij het tijdelijk verlaten van de werkplek, bijvoorbeeld door het tegelijkertijd intoetsen van de sneltoetsen Windows + L .
   
2. Voorkom dat gevoelige of vertrouwelijke informatie zichtbaar is wanneer iemand anders op het beeldscherm mee kan kijken. Sluit het e-mailprogramma af en zorg voor een opgeruimd digitaal bureaublad.

Gebruik eigen apparatuur

Beveiligingsmaatregelen hebben betrekking op alle apparaten waarmee werkzaamheden voor *[LVO/naam school]* worden uitgevoerd. *[LVO/naam school]* is verantwoordelijk voor het implementeren van de juiste beveiligingsmaatregelen als het gaat om de bedrijfsmiddelen van de school. Voor eigen apparaten ligt de verantwoordelijkheid voor adequate beveiligingsmaatregelen bij de medewerker zelf. Van de medewerker wordt verwacht dat minimaal de volgende beveiligingsmaatregelen worden genomen:

1. Beveilig het apparaat met een wachtwoord, of in het geval van een smartphone of tablet, met een pincode.
2. Vergrendel het apparaat bij het verlaten van de werkplek.
3. Sla persoonsgegevens van bij *[LVO/naam school*] betrokken personen niet op het eigen apparaat op. Dit is niet toegestaan.
4. Versleutel alle gegevens, anders dan persoonsgegevens, met betrekking tot *[LVO/naam school]* als deze, om welke reden dan ook, niet op het schoolnetwerk opgeslagen worden.
5. Maak op het eigen apparaat een duidelijke scheiding tussen de opslag van privégegevens en schoolgerelateerde gegevens, bijvoorbeeld door aanmaken van een folder genaamd ‘school’.
6. Houd software up-to-date door het uitvoeren van periodieke updates.
7. Neem adequate maatregelen tegen virussen of malware door het up-to-date houden van de virusscanner en door het periodiek scannen van het apparaat.
8. Op verzoek van *[LVO/naam school]* toont de medewerker aan dat hij bovenstaande maatregelen heeft toegepast. [*LVO/naam school*] zal bij controle op de beveiligingsmaatregelen uitgaan van de juiste balans tussen verantwoord gebruik en de bescherming van de privacy van medewerker. Controle op toepassing van de juiste beveiligingsmaatregelen vindt slechts plaats in het kader van handhaving van de doelen van dit protocol.

Software en digitaal lesmateriaal

Het gebruik van digitaal lesmateriaal is niet meer weg te denken bij *[LVO/naam school]*. Dit lesmateriaal staat steeds meer online waarbij steeds vaker persoonsgegevens worden uitgewisseld. De privacywetgeving eist dat elke organisatie vooraf aan het gebruik van dergelijk materiaal bekijkt wat de invloed ervan is op de privacy. Dit kan specifieke maatregelen tot gevolg hebben. De onderstaande regels gelden voor de installatie en het gebruik van software en (online) digitaal lesmateriaal:

1. Installeren van software wordt bij *[LVO/naam school]* alleen toegestaan met de juiste licenties en na het nemen van eventuele aanvullende maatregelen.
2. Bij het gebruik van online software, applicaties en digitaal lesmateriaal, wordt gekeken of er persoonsgegevens verwerkt worden.
3. Een verwerkersovereenkomst wordt vooraf aan het gebruik afgesloten met elke leverancier van (online) software, die in opdracht van *[LVO/naam school]* persoonsgegevens verwerkt.
4. Aanvragen van digitaal lesmateriaal en/of andere software gebeurt via de door *[LVO/naam school]* afgesproken aanvraagprocedure.

Gebruik van Microsoft Office 365 en schoolgerelateerde applicaties

[LVO/naam school] stelt Microsoft Office 365, een bijbehorende mailbox en applicaties (zoals Somtoday en itslearning) aan de medeweker ter beschikking voor het uitoefenen van de schoolwerkzaamheden. Gebruik van de Microsoft Office 365 faciliteiten en de applicaties is verbonden aan deze schoolwerkzaamheden en daarbij zijn de volgende regels van toepassing:

1. Gebruik de faciliteiten voor schoolgerelateerde zaken.

2. Gebruik voor privé communicaties een eigen e-mailadres via een externe webmaildienst of eigen provider.
3. Ontvangen van privémail op het e-mailadres van school is incidenteel toegestaan.
4. Het gebruik moet voldoen aan de normale gedragsregels die gelden op school.
5. Het is niet toegestaan om de hierboven genoemde faciliteiten te gebruiken voor berichten met pornografische, racistische, discriminerende, beledigende, (seksueel) intimiderende of aanstootgevende inhoud of voor berichten die kunnen aanzetten tot haat of geweld.
6. Synchroniseert een medewerker de school e-mail met eigen apparatuur (bijvoorbeeld een tablet of telefoon) dan kan *[LVO/naam school]*, bij verlies of diefstal van het device, gebruik maken van de mogelijkheid om de e-mail op afstand te wissen, ook als daarmee alle (privé)gegevens van het apparaat gewist worden.

Gebruik van het LVO-schoolnetwerk

Het gebruik van het LVO-netwerk en de bijbehorende faciliteiten op de scholen, het kantoor in Sittard of op de thuiswerkplek worden aan de medewerker voor het uitoefenen van zijn werkzaamheden beschikbaar gesteld. Gebruik hiervan is verbonden aan deze werkzaamheden en daarbij gelden de volgende regels:

1. Het LVO-netwerk is alleen toegankelijk voor geregistreerde gebruikers.
2. Medewerkers mogen alleen onder hun eigen naam en met hun eigen account gebruik maken van het netwerk. Na gebruik sluit de medewerker zijn eigen account ook weer af.
3. De gebruikersnaam en het bijbehorende wachtwoord zijn strikt persoonlijk en mogen niet aan anderen worden doorgegeven. Ditzelfde is van toepassing op alle door *LVO/naam school* verstrekte inloggegevens.
4. De medewerker dient bij (vermoeden van) misbruik van diens gegevens of bij (vermoeden van) inbreuken op de beveiliging van het netwerk, van binnenuit of van buiten LVO/de school, direct contact op te nemen met zijn/haar leidinggevende.
5. Het is de medewerker niet toegestaan om zich moedwillig toegang te verschaffen tot andermans gegevens of bestanden.
6. Onbedoelde inbreuk op beveiliging, van binnenuit of buiten LVO/de school dient onmiddellijk aan de leidinggevende gemeld te worden.

Gebruik van internet

[LVO/naam school] stelt het gebruik van internet en de bijbehorende faciliteiten aan de medewerker ter beschikking voor het uitoefenen van de werkzaamheden. Gebruik hiervan is verbonden aan deze werkzaamheden en daarbij zijn de volgende regels van toepassing:

1. Beperkt persoonlijk gebruik is toegestaan, mits dit:
   a. niet storend is voor de dagelijkse werkzaamheden;
   b. niet voor commerciële doeleinden is; en
   c. geen verboden gebruik oplevert.
2. Het is niet toegestaan om:
   a. op internet websites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten, tenzij het raadplegen ervan voor onderwijsactiviteiten noodzakelijk is;
   b. films, muziek, software en overig auteursrechtelijk beschermd materiaal (zoals foto's of teksten) te downloaden of te gebruiken zonder een vergoeding daarvoor te betalen aan de rechthebbenden;
   c. (kans)spellen te spelen en gamewebsites te bezoeken, tenzij dit als onderzoek wordt gedaan ter ondersteuning van een (te ontwikkelen) lesprogramma;
   d. onder werktijd internettoegang te gebruiken voor privédoeleinden.
3. Het is verboden op dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende toon te communiceren via online fora, sociale netwerken en andere vergelijkbare communicatienetwerken over alle aan LVO of de school verbonden betrokkenen en activiteiten. Dit geldt in het bijzonder ook voor internetgebruik buiten het LVO/netwerk met betrekking tot aan LVO of de school verbonden betrokkenen en activiteiten.

Veilig online

We brengen met z'n allen steeds meer tijd online door. Hierbij worden steeds meer mobiele apparaten gebruikt. Menselijk (online) handelen staat veelal aan de basis van een datalek. *[LVO/naam school]* verwacht van medewerkers dat zij:

1. Het onderscheid kennen tussen veilige en onveilige netwerken (openbare wifinetwerken) en websites.
2. Bij het verwerken van persoonsgegevens alleen gebruik maken van bekende en beveiligde draadloze netwerken.
3. Weten wat malware is, het kunnen herkennen en weten hoe te handelen. Medewerkers en leerlingen dienen alert te zijn op phishingmails en verdachte links en/of bijlagen en deze niet zomaar te openen.
4. Terughoudend zijn met het online achterlaten van gegevens met betrekking tot *[LVO/naam school]* met name bij niet schoolgerelateerde instanties.
5. Zeer terughoudend zijn in het gebruik van (beveiligde) netwerken in openbare ruimtes.

Controle gebruik internetfaciliteiten

1. *[LVO/naam school]* zal bij controle rondom het gebruik van de internetfaciliteiten op basis van dit protocol uitgaan van de juiste balans tussen verantwoord gebruik van de internetfaciliteiten en de bescherming van de privacy van medewerkers. Controle kan alleen plaatsvinden door de afdeling ICT en de systeembeheerder en vindt alleen plaats op een onderbouwd gezamenlijk verzoek aan de manager ICT door de voorzitter van het college van bestuur en de rector/locatiedirecteur/directeur ondersteunende diensten aan wie ook de bevindingen van de controle worden gerapporteerd.
2. Indien *[LVO/naam school]* tot controle overgaat, gelden de volgende voorwaarden:
   a. Controle van persoonsgegevens met betrekking tot gebruik van de internetfaciliteiten vindt slechts plaats in het kader van handhaving van de doelen van dit protocol.
   b. Controle vindt in beginsel plaats op het niveau van samengevoegde gegevens die niet herleidbaar zijn tot identificeerbare personen.
   c. Indien een medewerker of een groep medewerkers wordt verdacht van het overtreden van de regels, kan gedurende een vastgestelde (korte) periode, in opdracht van het college van bestuur gerichte controle plaatsvinden.
   d. Controle beperkt zich in beginsel tot verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen vindt, in opdracht van het college van bestuur, controle op de inhoud plaats.
   e. Verboden e-mail- en internetgebruik wordt zo veel mogelijk softwarematig onmogelijk gemaakt.
   f. Bij constatering van ongeoorloofd gebruik wordt dit onmiddellijk met de betrokken medewerker besproken. *[LVO/naam school]* zal de medewerker op verzoek inzage verschaffen in de gegevens over het eigen gebruik. De medewerker wordt gewezen op de consequenties wanneer niet gestopt wordt met het ongeoorloofd gebruik. In ernstige gevallen kan *[LVO/naam school]* direct sancties jegens de medewerker treffen.
   g. E-mailberichten van leden van de (G)MR die worden verstuurd in het kader van het uitoefenen van de (G)MR-functie , van interne vertrouwenspersonen en van eenieder die zich op grond van zijn functie op enige vertrouwelijkheid moet kunnen beroepen, worden in principe niet gecontroleerd. Dit geldt niet voor de veiligheid van berichten. Ook hier kan bij zwaarwegende redenen van afgeweken worden.
3. Bij de uitvoering van de controle gelden de volgende voorwaarden:
   a. De controle ter voorkoming van negatieve publiciteit en seksuele intimidatie en de controle in het kader van systeem- en netwerkbeveiliging vindt plaats op basis van content-filtering.
   b. De controle op het uitlekken van interne en vertrouwelijke gegevens vindt plaats op basis van steekproefsgewijze content-filtering. Verdachte berichten worden apart gezet voor nader onderzoek.
   c. De controle in het kader van kosten- en capaciteitsbeheersing wordt beperkt tot verkeers- en opslaggegevens.
   d. Controle op het gebruik van beeldmateriaal vindt plaats op basis van klachten of meldingen van derden, of steekproefsgewijs bij beeldmateriaal dat openbaar beschikbaar is.

e. De afdeling ICT en de systeembeheerder zijn aan geheimhouding gebonden als men om technische redenen kennis moet nemen van persoonsgebonden informatie, behalve als enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.
f. Door *[LVO/naam school]* worden de nodige maatregelen getroffen, opdat persoonsgegevens, gelet op de doeleinden waarvoor zij zijn verwerkt, juist en nauwkeurig zijn.
g. Door *[LVO/naam school]* worden passende technische en organisatorische maatregelen getroffen om persoonsgegevens te beveiligen tegen verlies en/of tegen enige vorm van onrechtmatige verwerking.

Voor leerlingen

Computergebruik

Computer- en/of netwerkfaciliteiten worden voor het uitoefenen van de schoolwerkzaamheden aan de leerling beschikbaar gesteld door *[LVO/naam school]*. Het gebruik van de computer- en/of internetfaciliteiten is verbonden aan deze schoolwerkzaamheden en daarbij gelden de volgende regels:

1. Het installeren van software op computers van *[LVO/naam school]* is niet toegestaan zonder toestemming van *[LVO/naam school]* en eventuele benodigde licenties.
2. Wachtwoorden zijn persoonlijk en worden niet gedeeld. Ook niet incidenteel.
3. De leerling logt uit na het gebruik van de computer.
4. Bij het tijdelijk verlaten van de werkplek vergrendelt de leerling de computer/laptop, bijvoorbeeld door het gelijktijdig indrukken van de sneltoetsen Windows + L. De laptop wordt niet onbeheerd achtergelaten.

5. Iedere leerling heeft de beschikking over eigen schijfruimte op Microsoft OneDrive om zijn/haar gegevens op te slaan.
6. Deze ruimte wordt regelmatig door de systeembeheerder gescand op de fysieke aanwezigheid van programma's en inhoudelijk op de aanwezigheid van bestanden met pornografische, racistische, discriminerende, gewelddadige of anderszins onacceptabele, dan wel niet voor het onderwijs aan *[LVO/naam school]* bestemde inhoud. De beoordeling hiervan ligt bij de schoolleiding.
7. Het is niet toegestaan bestanden van bovengenoemde aard te downloaden, op het netwerk te plaatsen, in bezit te hebben, te delen of van deze bestanden gebruik te maken. Dit geldt ook voor het openen van deze bestanden via externe drives.

Gebruik eigen apparatuur

Bij het gebruik van eigen apparatuur (zoals laptop, tablet of smartphone) op school dienen er een aantal beveiligingsmaatregelen genomen te worden. Als je een apparaat van school gebruikt, dan mag je ervan uitgaan dat *[LVO/naam school]* deze beveiligingsmaatregelen genomen heeft. Voor gebruik van de internetfaciliteiten met eigen apparatuur moeten minimaal de volgende beveiligingsmaatregelen genomen zijn:

1. Bescherm de toegang tot het apparaat met een wachtwoord of, in het geval van een tablet of smartphone met een pincode.
2. Zorg dat je apparaat vergrendeld is wanneer je er niet bij in de buurt bent, zodat niemand in jouw bestanden en gegevens kan.
3. Houd de software up-to-date door periodieke updates.
4. Neem goede maatregelen tegen virussen en malware, bijvoorbeeld door periodiek je apparaat te scannen.
5. Op verzoek van *[LVO/naam school]* toon je aan dat je bovenstaande maatregelen hebt toegepast. [*LVO/naam school*] zal bij controle op de beveiligingsmaatregelen uitgaan van de juiste balans tussen verantwoord gebruik en de bescherming van de privacy. Controle op toepassing van de juiste beveiligingsmaatregelen vindt slechts plaats in het kader van handhaving van de doelen van dit protocol.

Gebruik van Microsoft Office 365 en schoolgerelateerde applicaties

[LVO/naam school] stelt Microsoft Office 365, een bijbehorende mailbox en applicaties (zoals Somtoday en itslearning) aan de leerling ter beschikking voor het uitoefenen van de schoolwerkzaamheden. Gebruik van de Microsoft Office 365 faciliteiten en de applicaties is verbonden aan deze schoolwerkzaamheden en daarbij zijn de volgende regels van toepassing:

1. Gebruik de faciliteiten voor schoolgerelateerde zaken.
2. Gebruik voor privécommunicatie een eigen e-mailadres via een externe webmaildienst of een eigen provider.
3. Ontvangen van privémail op het school e-mailadres is incidenteel toegestaan.
4. De inhoud van de communicatie moet voldoen aan de normale gedragsregels die gelden op school.
5. Het is niet toegestaan om de hierboven genoemde faciliteiten te gebruiken voor berichten met pornografische, racistische, discriminerende, beledigende, (seksueel) intimiderende of aanstootgevende inhoud of voor berichten die kunnen aanzetten tot haat of geweld.

Gebruik van LVO-schoolnetwerk

Het gebruik van het schoolnetwerk en de bijbehorende faciliteiten worden aan de leerling voor het uitoefenen van de schoolwerkzaamheden op school beschikbaar gesteld. Gebruik hiervan is verbonden aan deze schoolwerkzaamheden en daarbij gelden de volgende regels:

1. Het schoolnetwerk is alleen toegankelijk voor geregistreerde gebruikers.
2. Leerlingen mogen alleen onder hun eigen naam en met hun eigen schoolaccount gebruik maken van het schoolnetwerk. Na gebruik sluit de leerling zijn eigen schoolaccount ook weer af.
3. De gebruikersnaam en het bijbehorende wachtwoord zijn strikt persoonlijk en mogen niet aan anderen worden doorgegeven. Ditzelfde is van toepassing op alle door de school verstrekte inloggegevens.
4. De leerling dient bij (vermoeden van) misbruik van zijn/haar gegevens, de gegevens van anderen of bij (vermoeden van) inbreuken op de beveiliging van het schoolnetwerk, van binnenuit of van buiten de school, direct contact op te nemen met zijn/haar mentor.
5. Het is de leerling niet toegestaan om zich moedwillig toegang te verschaffen tot andermans gegevens of bestanden.
6. Onbedoelde inbreuk op beveiliging, van binnenuit of buiten de school dient ook onmiddellijk aan de mentor gemeld te worden.

Gebruik van internet

[LVO/naam school] stelt het gebruik van internet en de bijbehorende faciliteiten aan de leerling ter beschikking voor het uitoefenen van de schoolwerkzaamheden. Gebruik hiervan is verbonden aan deze schoolwerkzaamheden en daarbij zijn de volgende regels van toepassing:

1. Internet wordt uitsluitend gebruikt voor schooldoeleinden.
2. Het is niet toegestaan om op internet websites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten.
3. Het is niet toegestaan om films, muziek, software en overig auteursrechtelijk beschermd materiaal (zoals foto's of teksten) te downloaden of te gebruiken zonder een vergoeding daarvoor te betalen aan de rechthebbenden.
4. Het is niet toegestaan om (kans)spellen te spelen en gamewebsites te bezoeken, anders dan in opdracht van en met toestemming van de docent of de systeembeheerder.
5. Het bezoeken van chatboxen of vergelijkbare toepassingen is alleen toegestaan in het kader van lesopdrachten.
6. Het is verboden op dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende toon te communiceren via online fora, sociale netwerken en andere vergelijkbare communicatienetwerken over alle aan school verbonden betrokkenen en activiteiten. Dit geldt in het bijzonder ook voor internetgebruik buiten het schoolnetwerk met betrekking tot personen en activiteiten die aan de school zijn verbonden.

Veilig online

We brengen steeds meer tijd online door. Hierbij worden steeds meer mobiele apparatuur gebruikt. Menselijk (online) handelen staat veelal aan de basis van een datalek. *[LVO/naam school]* verwacht van leerlingen dat zij:

1. Het onderscheid kennen tussen veilige en onveilige netwerken (openbare wifinetwerken) en websites.
2. Bij het verwerken van persoonsgegevens alleen gebruik maken van bekende en beveiligde draadloze netwerken.
3. Controleren of er daadwerkelijk van een bekend en beveiligd netwerk gebruik gemaakt wordt bij het bezoek aan openbare ruimtes.
4. Weten wat malware is, het kunnen herkennen en weten hoe te handelen.
5. Terughoudend zijn met het online achterlaten van gegevens met betrekking tot *[LVO/naam school]*.

Controle gebruik internetfaciliteiten

1. *[LVO/naam school]* zal bij controle rondom het gebruik van de internetfaciliteiten op basis van dit protocol uitgaan van de juiste balans tussen verantwoord gebruik van de internetfaciliteiten en de bescherming van de privacy van leerlingen. Controle kan alleen plaatsvinden door de afdeling ICT en de systeembeheerder en vindt alleen plaats op een onderbouwd gezamenlijk verzoek aan de manager ICT door de voorzitter van het college van bestuur en de rector/locatiedirecteur/directeur ondersteunende diensten aan wie ook de bevindingen van de controle worden gerapporteerd.
2. Indien *[LVO/naam school]* tot controle overgaat, gelden de volgende voorwaarden:
    a. Controle van persoonsgegevens met betrekking tot gebruik van de internetfaciliteiten vindt slechts plaats in het kader van handhaving van de doelen van dit protocol.
    b. Controle vindt in beginsel plaats op het niveau van verzamelde gegevens die niet herleidbaar zijn tot identificeerbare personen.
    c. Indien een leerling of een groep leerlingen wordt verdacht van het overtreden van de regels, kan gedurende een vastgestelde (korte) periode, in opdracht van *[LVO/naam school]* gerichte controle plaatsvinden.
    d. Controle beperkt zich in beginsel tot verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen vindt, in opdracht van *[LVO/naam school]*, controle op de inhoud plaats.
    e. Verboden e-mail- en internetgebruik wordt zo veel mogelijk softwarematig onmogelijk gemaakt.
    f. Bij constatering van ongeoorloofd gebruik wordt dit onmiddellijk met de betrokken leerling besproken. *[LVO/naam school]* zal de leerling op verzoek inzage verschaffen in de gegevens over het eigen gebruik. De leerling wordt gewezen op de consequenties wanneer niet gestopt wordt met het ongeoorloofd gebruik. In ernstige gevallen kan *[LVO/naam school]* direct sancties jegens de leerling treffen.
3. Bij de uitvoering van de controle gelden de volgende voorwaarden:
    a. De controle ter voorkoming van negatieve publiciteit en seksuele intimidatie en de controle in het kader van systeem- en netwerkbeveiliging vindt plaats op basis van content-filtering.
    b. De controle op het uitlekken van interne en vertrouwelijke gegevens vindt plaats op basis van steekproefsgewijze content-filtering. Verdachte berichten worden apart gezet voor nader onderzoek.
    c. De controle in het kader van kosten- en capaciteitsbeheersing wordt beperkt tot verkeers- en opslaggegevens.
    d. Controle op het gebruik van beeldmateriaal vindt plaats op basis van klachten of meldingen van derden, of steekproefsgewijs bij beeldmateriaal dat openbaar beschikbaar is.
    e. De afdeling ICT en de systeembeheerder zijn aan geheimhouding gebonden als men om technische redenen kennis moet nemen van persoonsgebonden informatie, behalve als enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.

f. Door *[LVO/naam school]* worden de nodige maatregelen getroffen, opdat persoonsgegevens, gelet op de doeleinden waarvoor zij zijn verwerkt, juist en nauwkeurig zijn.
g. Door *[LVO/naam school]* worden passende technische en organisatorische maatregelen getroffen om persoonsgegevens te beveiligen tegen verlies en/of tegen enige vorm van onrechtmatige verwerking.

Deel III: Gevolgen

Gevolgen voor leerlingen en ouders

1. Afhankelijk van de ernst van de uitingen en/of gedragingen van leerlingen en/of ouders en de gevolgen daarvan zullen er gepaste maatregelen worden genomen, die onder meer kunnen bestaan uit: een gesprek, het tijdelijk in bewaring nemen van devices, het (laten) verwijderen van berichten en/of beelden daarop, een waarschuwing, schorsing of verwijdering van school. Bij ernstige overtredingen zal de correspondentie in het leerlingdossier worden opgenomen.
2. Wanneer uitingen of gedragingen van leerlingen en/of ouders mogelijk een strafrechtelijke overtreding inhouden kan door *[LVO/naam school]* melding of aangifte bij de politie worden gedaan.

Gevolgen voor medewerkers

1. Medewerkers houden zich bij de vervulling van hun functie aan de regels die ten behoeve van de goede gang van zaken door *[LVO/naam school]* door middel van instructies en/of reglementen zijn vastgesteld, waaronder het onderhavige protocol.
2. Medewerkers die in strijd handelen met dit protocol maken zich mogelijk schuldig aan plichtsverzuim, zoals bedoeld in de vigerende CAO VO. Alle correspondentie ten aanzien van plichtsverzuim wordt opgenomen in het personeelsdossier van de betrokken medewerker.
3. Indien *[LVO/naam school]* de wijze van communiceren of het handelen door een medewerker jegens een leerling als grensoverschrijdend kwalificeert, dan wordt dit *altijd* telefonisch gemeld bij de Landelijke Vertrouwensinspecteur (0900-1113111). Als grensoverschrijdende gedragingen hebben in ieder geval (doch niet uitsluitend) te gelden intimiteiten met een leerling in geschrift, afbeelding, gebaar of aanraking dan wel het maken van seksueel getinte, racistische of discriminerende grappen of opmerkingen. In andere gevallen kan *[LVO/naam school]* de Vertrouwensinspecteur raadplegen.
4. Afhankelijk van de ernst van de uitingen en/of gedragingen van medewerkers en de gevolgen daarvan kunnen rechtspositionele maatregelen worden genomen die variëren van waarschuwing, berisping, schorsing, inhouding bezoldiging, ontslag en ontslag op staande voet.
5. Wanneer uitingen of gedragingen van medewerkers mogelijk een strafrechtelijke overtreding inhouden kan door *[LVO/naam school]* melding of aangifte bij de politie worden gedaan.

Deel IV Slotbepalingen

1. Onderhavig protocol wordt aan alle leerlingen en medewerkers ter beschikking gesteld. Het protocol kan via intranet worden geraadpleegd en het wordt herhaaldelijk onder de aandacht gebracht van de leerlingen (tijdens bijvoorbeeld een mentorles) en de medewerkers (bijvoorbeeld in een regulier werkoverleg).
2. In alle gevallen waarin dit protocol niet voorziet beslist het college van bestuur.
3. Het Protocol sociale media & internetfaciliteiten treedt in werking op de datum van vaststelling door het college van bestuur en is voor onbepaalde duur van kracht. Het onderhavig protocol vervangt het Protocol Sociale Media en de LVO-Gedragscode internetfaciliteiten, die komen te vervallen bij de inwerkingtreding van het onderhavig protocol.
4. Het Protocol sociale media & internetfaciliteiten wordt eenmaal in de vijf jaar, of zoveel eerder als nodig, geëvalueerd en, na eventuele wijzigingen, opnieuw vastgesteld.