Bijlage III.a Protocol voor het gebruik van e-mail en ICT (personeel)

Het Calvijn College wil als school staan op de grondslag van de Heilige Schrift, als het onfeilbare Woord van God, zoals daarvan belijdenis wordt gedaan in de Drie Formulieren van Enigheid, die we geheel en onvoorwaardelijk willen onderschrijven.
Deze grondslag vraagt op alle gebieden vertaling naar de dagelijkse praktijk. Dat zal niet alleen zichtbaar moeten zijn in de manier waarop we onderwijs geven en met jongeren om gaan, maar ook in de manier waarop we als personeelsleden met media om gaan. Uitgangspunt van dit reglement is enerzijds de grondslag van de school en anderzijds de technische mogelijkheden die de school het personeel wil bieden om in de dagelijkse praktijk te kunnen functioneren.

Naast dit protocol is in het kader van het gebruik van het netwerk van de school en de faciliteiten daaromheen een gebruikershandleiding beschikbaar, die door de afdeling ICT gemaakt wordt. Daarnaast is een notitie Beeldschermwerk beschikbaar, die onder verantwoordelijkheid van P&O gemaakt wordt. Het gaat hierbij om medewerkers die meer dan 60% van hun werktijd computergerelateerde werkzaamheden moeten verrichten en die voor een functieomvang van minimaal 0,8 fte aan onze school verbonden zijn.

Voor de leerlingen is een vergelijkbaar protocol opgesteld en gepubliceerd als bijlage 3b.

Artikel 1 Werkingssfeer van deze regeling, begrippen

1.1 Deze regeling geeft de wijze aan waarop binnen de Stichting Calvijn College 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.

1.2 Deze regeling geldt voor een ieder die ten behoeve van de school werkzaamheden verricht (personeelsleden, maar bijvoorbeeld ook: stagiaires en vrijwilligers). 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 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 een device van school, het e-mailadres van de school of de schoolwebsite) zijn de bepalingen van deze regeling eveneens van toepassing.

1.5 Ten aanzien van de inrichting van het computernetwerk van de school en de daarop opererende systemen is de grootste zorgvuldigheid betracht, zodat de betrouwbaarheid daarvan maximaal gewaarborgd is. Voor eventuele problemen die zich zouden kunnen voordoen of voor eventuele schade die hieruit desondanks zou kunnen voortvloeien, accepteert de school geen aansprakelijkheid.

Artikel 2 Toegang tot en gebruik van de ICT

2.1 De Stichting Calvijn College 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 Bij constatering en misbruik van de faciliteiten of indien het gebruik ervan in de strijd is met dit reglement of met de wettelijke bepalingen, wordt toegang van de gebruiker die verantwoordelijk is voor het misbruik onmiddellijk ingetrokken, zodat deze geen toegang heeft tot het netwerk. Dit wordt door het Hoofd ICT&Planning gemeld aan de betrokkene en diens leidinggevende.

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

2.4 De gebruiker wordt geacht na eerste inlog het verstrekte wachtwoord te wijzigen in een veilig wachtwoord van 8 karakters in een combinatie van tenminste 2 cijfers en 4 letters en minstens eenmaal per jaar dit wachtwoord te wijzigen. Deze inloggegevens worden gebruikt voor zowel het netwerk als het portaal. Deze inlog is ook van toepassing voor Magister en Afas. Hier gelden dezelfde regels voor.

2.5 Bij constatering van misbruik van de betreffende combinatie dient de gebruiker de afdeling systeembeheer hiervan onverwijld op de hoogte te stellen.

2.6 De gebruiker dient alle redelijke maatregelen te nemen ter beveiliging van zijn inloggegevens.

2.7 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.

2.8 Gebruikers ontvangen een chippas ten behoeve van printen en kopiëren met apparatuur van de Stichting. Het verlies van de chippas dient direct gemeld te worden bij de afdeling systeembeheer. Binnen drie dagen zal een nieuwe pas verstrekt worden.

2.9 Personeelsleden kunnen op school afdrukken maken via printen en kopiëren. Hiervoor geldt een maximum per dag van 100 afdrukken in totaal. Grotere opdrachten moeten bij de externe repro aangeboden worden. Privé afdrukken of kopieën mogen gemaakt worden. Deze moeten op een apart budget geboekt worden en zullen eenmaal per kwartaal afgerekend worden tegen de tarieven die op het portaal vermeld staan.

2.10 Voor het opslaan van bestanden heeft elk personeelslid de beschikking over een OneDrive. Deze is op apparaten van de school te vinden onder ‘OneDrive Calvijn College’ in de Verkenner. Hierin worden **persoonlijke** bestanden opgeslagen. Alle bestanden die te maken hebben met de functie van het personeelslid behoren in het SharePoint of in een Teams omgeving opgeslagen te worden.

Artikel 3 Gebruik van de ICT-apparatuur

3.1 Vanaf het moment waarop aan de gebruiker een toegangscode en wachtwoord wordt verstrekt, is de gebruiker aansprakelijk voor de handelingen en eventuele daarmee verbonden gevolgen die voortvloeien uit zijn gebruik van de combinatie van toegangscode en wachtwoord.

3.2 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.

3.3 Tijdens het gebruik van de ICT-apparatuur is het niet toegestaan etens- en drinkwaren te nuttigen.

3.4 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.

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

3.6 Het gebruik van eigen opslagmedia (bijvoorbeeld: een USB-stick) van de gebruikers is niet toegestaan.

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

a) Er wordt geen toegang gegeven tot het netwerk van de school. Er kan uitsluitend gebruik gemaakt worden van de gasten-wifi (CC_eigen_device). Hierop kunnen geen interne bronnen geraadpleegd worden en kan geen gebruik gemaakt worden van de printers.

b) Op het eigen apparaat mag geen data van het Calvijn College lokaal opgeslagen worden.

c) Gegevens van de school kunnen online geraadpleegd worden in Microsoft365.

3.8 Ten aanzien van de hoeveelheid opslagruimte op de persoonlijke drive en in de persoonlijke mailbox gelden door Hoofd ICT&Planning vastgestelde maxima.

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

4.1 De Stichting Calvijn College beperkt de toegang tot bepaalde sites door middel van een filtersysteem.

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. Wanneer deze extern verzonden wordt, mag dat uitsluitend door gebruik te maken van beveiligde email door het onderwerp te laten beginnen met de letters VM en een dubbele punt, VM:

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 applicaties buiten Microsoft365 van het Calvijn College (zoals Gmail, Hotmail, Dropbox, Whatsapp, WeTransfer of anders-

zins) kan leiden tot doorgifte van Persoonsgegevens buiten de EER verbiedt de Stichting Calvijn College het gebruik van deze software en diensten door medewerkers.

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 melden gesignaleerde zwakke plekken in de systemen, zodat zo snel mogelijk maatregelen kunnen worden getroffen. Melding kan worden gedaan bij de teamleider systeembeheer.

5.4 Vanaf het moment dat aan de gebruiker een toegangscode en wachtwoord wordt verstrekt en daarmee toegang tot het computernetwerk, wordt de gebruiker geacht deel te nemen aan de binnen de school opgezette mededelingen of verzoeken die via de e-mail of het portaal worden gedaan. Uitgangspunt is dat een personeelslid tenminste elke werkdag eenmaal zijn e-mail controleert en kennis neemt van de mededelingen op het portaal.

Onverantwoord gebruik

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

5.6 Het is niet toegestaan zich toegang te verschaffen tot gegevens van andere gebruikers.

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

5.8 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 die het systeem negatief beïnvloeden;

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 chatvoorzieningen, anders dan door de Stichting Calvijn College toegelaten chatvoorzieningen in Microsoft365 en voor schooldoeleinden;
n) acties te verrichten die ingaan tegen de wet.

5.9 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.

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

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

5.12 Voor personeelsleden is het op hun eigen apparaat toegestaan software lokaal te installeren die nodig is voor de werkzaamheden ten behoeve van school.

5.13 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.

5.14 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 De school behoudt zich het recht voor alle op het computernetwerk en de daarmee verbonden systemen verrichte acties te registreren.

6.3 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 het College van Bestuur.

6.4 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.

6.5 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 Richtlijnen voor contact middels ICT

9.1 Onderlinge berichten met een uitsluitend privé-inhoud, die geen link hebben met het onderwijs of de professionele relatie tussen personeelsleden en leerlingen, binnen dan wel buiten schooltijd, door middel van e-mail en andere media (bijvoorbeeld via Whatsapp) is in beginsel verboden.

9.2 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 teamleider van de leerling. Het personeelslid mag het contact met de leerling uitsluitend onderhouden via het e-mailadres van de school.

9.3 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.

9.4 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.

9.5 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 Stichting.

Artikel 10 Disciplinaire maatregelen bij leerlingen

10.1 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.

Artikel 11 Disciplinaire maatregelen bij personeelsleden

11.1 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.

11.2 Wanneer een gebruiker zich niet houdt aan de in dit reglement gegeven voorschriften kan hij uitgesloten worden van toegang tot het netwerk of delen daarvan.

Bijlage III.b Protocol voor het gebruik van e-mail en ICT (leerlingen)

Het Calvijn College wil als school staan op de grondslag van de Heilige Schrift, als het onfeilbare Woord van God, zoals daarvan belijdenis wordt gedaan in de Drie Formulieren van Enigheid, die we geheel en onvoorwaardelijk willen onderschrijven.
Deze grondslag vraagt op alle gebieden vertaling naar de dagelijkse praktijk. Dat zal niet alleen zichtbaar moeten zijn in de manier waarop onderwijs geven wordt en met elkaar wordt om gaan, maar ook in de manier waarop we met media om gaan. Uitgangspunt van dit reglement is enerzijds de grondslag van de school en anderzijds de technische mogelijkheden die de school de leerlingen wil bieden om in de dagelijkse praktijk te kunnen functioneren.

Artikel 1 Werkingssfeer van deze regeling, begrippen

1.1 Deze regeling geeft de wijze aan waarop binnen de Stichting Calvijn College 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.

1.2 Deze regeling geldt voor een ieder die onderwijs volgt (leerlingen). In dit reglement worden zij 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 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 (en de daarmee verbonden systemen en faciliteiten) zijn de bepalingen van deze regeling eveneens van toepassing.

Artikel 2 Toegang tot en gebruik van de ICT

2.1 De Stichting Calvijn College 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.

2.4 Gebruikers ontvangen een chippas ten behoeve van printen en kopiëren met apparatuur van de Stichting. Het verlies van de chippas dient direct gemeld te worden bij de mediatheek.

2.5 Leerlingen kunnen op school afdrukken maken via printen en kopiëren. De kosten hiervan zijn voor rekening van de leerling.

2.6 Voor het opslaan van bestanden heeft elke leerling de beschikking over een OneDrive. Deze is op het schoolnetwerk te bereiken onder OneDrive Calvijn College in de Verkenner en online in Microsoft365. Hierin worden **persoonlijke** bestanden opgeslagen.

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 verantwoorelijke docent of aan de beheerder van de mediatheek.

3.2 Tijdens het gebruik van de ICT-apparatuur is het niet toegestaan etens- en drinkwaren te nuttigen.

3.3 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.

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

3.5 Het gebruik van eigen opslagmedia (bijvoorbeeld: een USB-stick) van de gebruikers is niet toegestaan.

3.6 Het gebruik van eigen computerapparatuur (bijvoorbeeld laptops of tablets) is binnen de school niet toegestaan, behalve met toestemming van de locatiedirecteur.

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

4.1 De Stichting Calvijn College 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;

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.

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 opleiding van de leerling.

5.2 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 melden gesignaleerde zwakke plekken in de systemen, zodat zo snel mogelijk maatregelen kunnen worden getroffen. Melding kan worden gedaan bij de teamleider systeembeheer via systeembeheer@calvijncollege.nl.

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.

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 die het systeem negatief beïnvloeden;

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 chatvoorzieningen, anders dan door de Stichting Calvijn College toegelaten chatvoorzieningen in Microsoft365 en voor schooldoeleinden;

n) acties te verrichten die ingaan tegen de wet.

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 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.

5.12 Als een leerling eraan twijfelt of een bepaald gebruik van ICT wel verantwoord is, dan overlegt hij daarover met de mediathecaris van de locatie.

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 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 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.

6.3 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.

6.4 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.

6.5 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.

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) de systeem- en netwerkbeveiliging;
- d) 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 5.12.

7.3 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).

7.4 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.

7.5 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 Richtlijnen voor contact middels ICT

9.1 Onderlinge berichten met een uitsluitend privé-inhoud, die geen link hebben met het onderwijs, binnen dan wel buiten schooltijd, door middel van e-mail en andere media (bijvoorbeeld via Whatsapp, Chats in Teams e.d.) is in beginsel verboden.

9.2 Het is niet toegestaan mailings te versturen aan groepen (mede-)leerlingen en andere groepen (al dan niet binnen de school), noch per mail noch met chats of anderszins in de schoolomgeving zonder voorafgaande toestemming van de teamleider.

Artikel 10 Disciplinaire maatregelen bij leerlingen

10.1 Indien door de schoolleiding wordt vastgesteld dat een leerling onverantwoord gebruik heeft gemaakt van de ICT of zich niet aan de richtlijnen gehouden heeft, 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 of maatregel.

Bijlage III.c Protocol sociale media

Inleiding

Sociale media vormen een verzamelbegrip voor online platforms waar de gebruikers, zonder of met minimale tussenkomst van een professionele redactie, de inhoud verzorgen. Onder de noemer sociale media worden onder andere weblogs of blogs, WhatsApp, videosites als YouTube en sociale netwerken als Facebook, Twitter en Instagram geschaard. Via deze media worden verhalen, kennis, ervaringen en beeld en/of geluidmateriaal gedeeld.

Sociale media bieden de mogelijkheid om te laten zien dat je trots bent op je school en kunnen een bijdrage leveren aan een positief imago van [naam onderwijsinstelling]. Van belang is te beseffen dat je met berichten op sociale media (onbewust) de goede naam van de school en betrokkenen ook kunt schaden. Om deze reden dient bewust met de sociale media omgegaan te worden.

Essentieel is dat de onderwijsinstellingen en de gebruikers van sociale media tegenover alle betrokkenen de reguliere fatsoensnormen in acht blijven nemen.

Het Calvijn College vindt het noodzakelijk dat haar medewerkers, leerlingen, ouders/verzorgers en andere betrokkenen verantwoord omgaan met sociale media en heeft dit protocol opgesteld om een ieder die bij het Calvijn College betrokken is of zich daarbij betrokken voelt daarvoor richtlijnen te geven.

Uitgangspunten

1. Het Calvijn College onderkent het belang van sociale media.
2. Dit protocol draagt bij aan een goed en veilig school- en onderwijsklimaat;
3. Dit protocol bevordert dat de instelling, medewerkers, leerlingen en ouders op de sociale media communiceren in het verlengde van de missie en visie van de onderwijsinstelling en daarbij de reguliere fatsoensnormen in acht nemen. Dit betekent dat we respect voor de school en elkaar hebben, dat we verdraagzaam zijn en iedereen in zijn[1] waarde laten;
4. De gebruikers van sociale media dienen rekening te houden met de goede naam van de school en van een ieder die betrokken is bij de school; medewerkers hebben hierbij een voorbeeldfunctie.
5. Het protocol dient ervoor alle betrokkenen bij de onderwijsinstelling, te beschermen tegen de mogelijke negatieve gevolgen van de sociale media;

Doelgroep en reikwijdte

1. Deze richtlijnen zijn bedoeld voor alle betrokkenen die deel uitmaken van de schoolgemeenschap, dat wil zeggen medewerkers, leerlingen, ouders/verzorgers en mensen die op een andere manier verbonden zijn aan het Calvijn College.
2. De richtlijnen in dit protocol hebben betrekking op berichten die direct of indirect gerelateerd zijn aan de school of wanneer sprake is een overlap is tussen school, werk en privé.

[1] Voor de leesbaarheid is in de tekst de 'hij' vorm gebruikt. Waarin 'hij' of 'zijn'' staat, kan ook 'zij' of 'haar' worden gelezen.

Sociale media, de Algemene Verordening Gegevensbescherming (AVG) en de school

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

1. Het is medewerkers en leerlingen niet toegestaan om tijdens de lessen actief te zijn op sociale media dan wel beeld en/of geluidsopnamen te maken en/of te verspreiden, tenzij door de schoolleiding respectievelijk leraren hiervoor vooraf toestemming is gegeven.
2. Het is betrokkenen toegestaan om kennis en informatie over school en de leden van de schoolgemeenschap te delen, mits het geen persoonsgegevens[2] betreft en andere betrokkenen niet schaadt.
3. De betrokkene is persoonlijk verantwoordelijk voor de inhoud die hij publiceert op de sociale media.
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. De onderwijsinstelling vraagt aantoonbaar schriftelijke toestemming aan medewerkers, ouders of aan leerlingen van 16 jaar en ouder om foto-, film- en geluidsopnamen van aan school gerelateerde situaties, waarop zij zijn afgebeeld, op de school- en/of persoonlijke sociale media te zetten.
6. Het is medewerkers niet toegestaan om met een privéaccount 'vrienden' te worden van leerlingen en ouders op sociale media.
7. Het is ouders en leerlingen niet toegestaan om opnames te maken van lessen op afstand en deze te delen op sociale media.
8. Iedereen neemt de reguliere fatsoensnormen tegenover betrokkenen van de onderwijsinstelling in acht. Indien handelingen worden verricht die in strijd zijn met de reguliere fatsoensnormen en/of (mogelijk) een strafbaar karakter hebben (bijvoorbeeld: hacken van een account, radicalisering, sexting, pesten, stalken, bedreigen, het verspreiden van memes of anderszins beschadigen) dan neemt de onderwijsinstelling passende maatregelen[3].
9. Indien een betrokkene kennis heeft van ontoelaatbare en/of grensoverschrijdende communicatie in woord, beeld en/of geluid dan dient hij dat te melden bij de schoolleiding of het bestuur.

B. Voor medewerkers tijdens werksituaties

1. Een medewerker kan in Microsoft Teams via Posts berichten maken ten behoeve van leerlingen van de klas waaraan hij lesgeeft. Dit ten behoeve van het door hem doorgeven van bijzondere aangelegenheden zoals bij voorbeeld lesuitval, het opgeven van huiswerk, het herinneren aan de gymspullen, schoolreisje, schoolkamp. Voor het maken van dit soort aan de school gelieerde groepen **mag geen gebruik** gemaakt worden van een openbaar medium buiten beheer van de school zoals Whatsapp.
   Die leerlingen, die om welke reden dan ook geen deel uit kunnen maken van deze groep, worden door de medewerker via de mail, post of op een andere wijze op de hoogte gesteld.

[2] „Persoonsgegevens": alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon (artikel 4 AVG).

[3] Zie ook: sancties en gevolgen voor medewerkers en leerlingen.

2. Medewerkers hebben een bijzondere verantwoordelijkheid bij het gebruik van sociale media: privémeningen van medewerkers kunnen eenvoudig verward worden met de officiële standpunten van de onderwijsinstelling.
   Indien een medewerker deelneemt aan een discussie die (op enigerlei wijze) te maken heeft met het Calvijn College dient de medewerker te vermelden dat hij medewerker is van het Calvijn College en welke functie hij heeft.
3. Als online communicatie dreigt te ontsporen dient de medewerker direct contact op te nemen met zijn leidinggevende om de te volgen strategie te bespreken.
4. Bij twijfel of een publicatie in strijd is met deze richtlijnen neemt de medewerker contact op met zijn leidinggevende.

C. Voor medewerkers tijdens privésituaties

1. Het is de medewerker toegestaan om school/werk gerelateerde onderwerpen te publiceren mits het geen persoonsgegevens die de school, haar medewerkers, leerlingen, ouders/verzorgers en andere betrokkenen betreft. Ook mag de publicatie de naam van de school niet schaden.
2. Het is voor medewerkers niet toegestaan standpunten en/of overtuigingen uit te dragen die in strijd zijn met de missie en visie van het Calvijn College en de uitgangspunten van dit protocol.
3. Indien de medewerker deelneemt aan een discussie die (op enigerlei wijze) te maken heeft met de onderwijsinstelling dient hij te vermelden dat hij medewerker is van het Calvijn College.
4. Als de medewerker over het Calvijn College publiceert dient hij het bericht te voorzien van de mededeling dat de standpunten en meningen in dit bericht de eigen persoonlijke mening zijn (op persoonlijke titel zijn geschreven) en los staan van eventuele officiële standpunten van het Calvijn College.

Sancties en gevolgen voor medewerkers en leerlingen

1. Medewerkers houden zich bij de vervulling van hun functie aan de regels die ten behoeve van de goede gang van zaken door de werkgever door middel van instructies en/of reglementen zijn vastgesteld[4] en hem door werkgever zijn verstrekt, waaronder het protocol sociale media en het Privacyreglement.
2. Medewerkers die in strijd handelen met dit protocol maken zich mogelijk schuldig aan plichtsverzuim. Alle correspondentie over dit onderwerp wordt opgenomen in het personeelsdossier.
3. Indien het Calvijn College de wijze van communiceren door een medewerker(s) als ‘grensoverschrijdend’ kwalificeert, dan wordt dit telefonisch gemeld bij de Landelijke Vertrouwensinspecteur (0900 – 1113111).
4. Afhankelijk van de ernst van de uitingen en/of gedragingen van medewerkers en de gevolgen daarvan worden rechtspositionele maatregelen genomen die variëren van waarschuwing, schorsing, berisping, ontslag en ontslag op staande voet.
5. Leerlingen en / of ouders/verzorgers die in strijd met dit protocol handelen maken zich mogelijk schuldig aan verwijtbaar gedrag. Alle correspondentie over dit onderwerp wordt opgenomen in het leerlingendossier.
6. Afhankelijk van de ernst van de uitingen en/of gedragingen van leerlingen en/of ouders/verzorgers en de gevolgen daarvan worden jegens hen maatregelen genomen die

[4] Zie artikel 11.2 lid 2 CAO PO en artikel 18.2 lid 2 CAO VO.

onder meer kunnen bestaan uit: het in bewaring nemen van devices, het verwijderen van berichten en/of beelden daarop, een waarschuwing, schorsing en verwijdering van school.

7. Wanneer uitingen of gedragingen van leerlingen en/of ouders/verzorgers dan wel medewerkers mogelijk een strafrechtelijke overtreding inhouden kan door het Calvijn College melding of aangifte bij de politie worden gedaan.

Dit protocol is in het kader van het vaststellen dan wel wijzigen van veiligheidsbeleid na instemming van de MR op 02-06-2021 door het bestuur vastgesteld op 02-06-2021.