**Verantwoord netwerk gebruik**

****

**IBPDOC26**

Verantwoording

**Bron:**

**Starterkit Informatiebeveiliging**

*Stichting SURF, Februari 2015*

**Regelement verantwoord netwerk gebruik, ROC West Brabant**

**J***an van den Hazelkamp, juni 2016*

**SCIPR**

SCIPR is een community of practice binnen de SURF samenwerkingsorganisatie met als doelen het actief stimuleren van en richting geven aan informatiebeveiliging en privacy binnen het hoger onderwijs en onderzoek (universiteiten, hogescholen, wetenschappelijk onderzoek en universitair medische centra). Dat wordt bereikt door het bevorderen van de samenwerking tussen informatiebeveiligers/kwartiermakers ib en privacy en het leveren van praktisch bruikbare adviezen.

Voor meer informatie zie [www.scipr.nl](http://www.scipr.nl)

**Bewerkt door:**

Kennisnet / saMBO-ICT

**Auteurs**

Jan van den Hazelkamp (ROC West Brabant)

Ludo Cuijpers (Kennisnet)

Leo Bakker (Kennisnet)

Versie 2.0, september 2017

**Sommige rechten voorbehouden**

Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, aanvaarden de auteur(s), redacteur(s) en uitgever van Kennisnet geen aansprakelijkheid voor eventuele fouten of onvolkomenheden.

**Creative commons**

Naamsvermelding 3.0 Nederland

(CC BY 3.0)

**De gebruiker mag:**

* Het werk kopiëren, verspreiden en doorgeven
* Remixen – afgeleide werken maken

**Onder de volgende voorwaarde:**

* Naamsvermelding – De gebruiker dient bij het werk de naam van Kennisnet te vermelden (maar niet zodanig dat de indruk gewekt wordt dat zij daarmee instemt met uw werk of uw gebruik van het werk).

# Inleiding

Het oorspronkelijke document, genaamd Acceptable Use Policy IBPDOC26, vs 1.0 gaf eigenlijk alleen de links weer naar de documenten die bij SCIPR gebruikt worden in het kader van verantwoord netwerk gebruik. Deze verwijzingen zijn aan het eind van dit document nog steeds opgenomen.

Maar intussen zijn er in het mbo veld op diverse plekken ook documenten ontwikkeld die voor het mbo heel geschikt zijn. daarom is voor het issue van verantwoord netwerk gebruik de documentatie van het ROC West Brabant met toestemming gegeneraliseerd en in dit document opgenomen als een heel goed voorbeeld voor hoe dat regelement eruit kan zien. Instellingen kunnen hier goed gebruik van maken.

Het reglement bestaat uit twee onderdelen, een voor deelnemers (studenten) en een voor medewerkers.

## Reglement Verantwoord Netwerkgebruik deelnemers

[Instelling], hierna te noemen de Instelling, biedt aan de eigen deelnemers en aan bezoekende deelnemers de mogelijkheid internet te gebruiken ten behoeve van de studie. Tevens worden aan deelnemers voor persoonlijk gebruik een instellingsgebonden mailbox en mogelijkheden tot opslag van bestanden en persoonlijke studiegegevens beschikbaar gesteld ten behoeve van de studie. Aan het gebruik van deze faciliteiten zijn regels verbonden.

### Gebruik van faciliteiten

Computer- en netwerkfaciliteiten (zoals openbare computers, draadloze en bedrade netwerkaansluitingen, e-mail en internettoegang, opslagcapaciteit, printers en elektronische leeromgevingen) worden aan de deelnemer beschikbaar gesteld, onder meer voor het kunnen maken van opdrachten, verslagen en werkstukken, het bijhouden van de studievoortgang, het raadplegen van bronnen en het communiceren met docenten en mededeelnemers.

Het gebruik van eigen apparatuur en toepassingen op de faciliteiten van de Instelling is toegestaan zolang dit gebruik voldoet aan de regels van dit Reglement. Het veranderen van instellingen in apparatuur en toepassingen beschikbaar gesteld door de Instelling is alleen toegestaan met aparte toestemming van de ict-beheerder. Het aansluiten van eigen netwerkapparatuur waarmee de verbinding kan worden gedeeld met derden op de bedrade of draadloze netwerkaansluitingen, is te allen tijde verboden.

Bepaalde faciliteiten zijn alleen toegankelijk met behulp van een gebruikersnaam en wachtwoord. Deze zijn persoonsgebonden en mogen niet met anderen worden gedeeld. De ict-beheerder kan nadere eisen stellen aan de kwaliteit van wachtwoorden en andere beveiligingsaspecten. Bij een vermoeden van misbruik van een wachtwoord kan de ict-beheerder per direct het betreffende account ontoegankelijk maken.

### Intellectueel eigendom en vertrouwelijke informatie

De deelnemer maakt geen inbreuk op de intellectuele eigendomsrechten van de Instelling en derden en respecteert de licentieafspraken zoals die van toepassing zijn binnen de Instelling. De zeggenschap over de informatie van de Instelling berust bij Instelling. De deelnemer heeft geen zelfstandige zeggenschap over de informatie behalve als hem dat expliciet is toegekend door de Instelling.

Indien de deelnemer in het kader van zijn studie of het uitvoeren van taken voor de Instelling toegang krijgt tot vertrouwelijke informatie of privacy gevoelige informatie waaronder persoonsgegevens, dient de deelnemer die informatie strikt vertrouwelijk te behandelen.

**Zie ook privacy reglement deelnemers.**

De deelnemer besteedt bijzondere aandacht aan het treffen van maatregelen zoals in dit Reglement genoemd, indien in het kader van het uitvoeren van deze taken de verwerking van vertrouwelijke informatie buiten de Instelling noodzakelijk is zoals via e-mail, in niet instellingsgebonden Cloud-toepassingen, op externe opslagmedia of eigen client-apparatuur (USB-apparaten, Tablets, etc.).

Indien de Instelling met betrekking tot het waarborgen van de vertrouwelijkheid en de intellectuele eigendomsrechten voorschriften heeft opgesteld, dient de deelnemer deze stipt op te volgen.

### Beveiliging door de Instelling én de deelnemer

De Instelling neemt informatiebeveiliging serieus. Zij hanteert dan ook een streng beveiligingsbeleid en neemt adequate technische en organisatorische maatregelen om de infrastructuur te beveiligen tegen verlies, diefstal, criminele activiteiten, verlies van vertrouwelijkheid, schending van privacy-rechten en schending van intellectuele eigendomsrechten.

Natuurlijk is een perfecte beveiliging onmogelijk. Daarom verwacht de Instelling ook van

deelnemers een proactieve houding en serieuze stappen om de eigen computer en andere apparatuur (zoals smartphones of tablets) adequaat te beveiligen. Zo is de deelnemer te allen tijde zelf verantwoordelijk voor het gebruik van de eigen apparatuur en de op deze apparatuur opgeslagen gegevens.

In het bijzonder dient de deelnemer, indien met zijn apparatuur gebruikt wordt gemaakt van de instellingsfaciliteiten, in het kader van beveiliging:

* deze apparatuur te voorzien van een adequate virusscanner en firewall;
* regelmatig reserve kopieën te maken van alle relevante data en kopieën van data veilig op te slaan;
* moeilijk te raden wachtwoorden te gebruiken en deze regelmatig te veranderen;
* deze apparatuur up-to-date te houden wat betreft software-instellingen.

### Privégebruik en overlast

Beperkt privégebruik van de faciliteiten is toegestaan. Gebruik, privé of voor studie, mag niet storend zijn voor de goede orde bij de Instelling en mag geen overlast veroorzaken bij anderen, inbreuk maken op rechten van de Instelling of derden of de integriteit en de veiligheid van het netwerk aantasten.

Onder storend en/of overlast veroorzakend gebruik wordt in ieder geval verstaan:

* het raadplegen van internetdiensten met een pornografische, racistische, discriminerende, beledigende of aanstootgevende inhoud of het verzenden van berichten met een dergelijke inhoud;
* het verzenden van berichten met een (seksueel) intimiderende inhoud of van berichten die (kunnen) aanzetten tot discriminatie, haat en/of geweld;
* het versturen van berichten aan grote aantallen ontvangers tegelijk, het versturen van kettingbrieven of het verspreiden van kwaadaardige software zoals virussen, wormen, Trojaanse paarden en spyware;
* filesharing- of streamingdiensten (zoals internetradio of Uitzendinggemist) te gebruiken wanneer dit overmatig veel dataverkeer genereert, zodanig dat het de beschikbaarheid van de faciliteiten in gevaar kan brengen;
* films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van enige illegale bron of wanneer de deelnemer weet/moet weten dat dit in strijd met auteursrechten is;
* films, muziek, software en overig auteursrechtelijk beschermd materiaal te verspreiden (uploaden) naar derden zonder toestemming van de rechthebbenden.

Het gebruik van computer- en netwerkfaciliteiten voor commerciële activiteiten is uitsluitend toegestaan wanneer de Instelling hiervoor schriftelijk toestemming heeft verleend.

### Monitoring door de Instelling

Controle van gebruik van de faciliteiten vindt slechts plaats in het kader van handhaving van de regels uit dit Reglement ten behoeve van de goede orde op de Instelling en de bewaking van de integriteit en de veiligheid van het netwerk en de computerfaciliteiten van de Instelling. Verboden gebruik van de faciliteiten wordt zo veel mogelijk langs technische weg onmogelijk gemaakt.

Voor deze controle worden geautomatiseerd gegevens verzameld (gelogd). Deze gegevens zijn alleen toegankelijk voor de direct verantwoordelijke systeembeheerders en worden alleen in geanonimiseerde vorm aan overige beheerders en andere verantwoordelijken beschikbaar gesteld. Deze kunnen tot nadere technische maatregelen besluiten, zoals een blokkade van de toegang tot een bepaalde dienst of het beperken van de mogelijkheden van het apparaat in kwestie om het netwerk te kunnen gebruiken.

In het bijzonder kan bij overlast, veroorzaakt door apparatuur van deelnemers, worden overgegaan tot uitschakeling van de netwerktoegangsmogelijkheden. Indien mogelijk wordt de deelnemer vooraf gewaarschuwd, zodat hij de gelegenheid heeft de overlast te staken. Wanneer dit wegens de vereiste spoed niet voorafgaand aan het nemen van de maatregel mogelijk is, doet de directeur (MBO) zo snel mogelijk melding van de maatregel.

Bij vermoedens van overtreding van de regels kan controle worden uitgevoerd op het niveau van individuele verkeersgegevens van het gebruik van de faciliteiten. Slechts bij zwaarwegende redenen vindt controle op de inhoud plaats.

De Instelling houdt zich bij het controleren op het niveau van verkeersgegevens of de inhoud onverkort aan de Wet bescherming persoonsgegevens en andere relevante regelgeving. In het bijzonder beveiligt de Instelling de bij controle vastgelegde gegevens tegen ongeautoriseerde toegang en worden personen met toegang daartoe contractueel verplicht tot geheimhouding.

### Procedure bij gericht onderzoek

Van gericht onderzoek is sprake wanneer verkeersgegevens of andere persoonsgegevens van de deelnemer worden vastgelegd in het kader van een onderzoek naar aanleiding van een zwaarwegend vermoeden van een overtreding van dit Reglement door die deelnemer.

Gericht onderzoek vindt uitsluitend plaats na schriftelijke opdracht van de directeur van de school, waarbij de reden vermeld zal worden waarom tot dit gerichte onderzoek zal worden overgegaan. De Raad van Bestuur ontvangt een afschrift van deze opdracht en een vastlegging van de resultaten van het onderzoek.

Gericht onderzoek beperkt zich in eerste instantie tot verkeersgegevens van het gebruik van de faciliteiten. Als gericht onderzoek nader bewijs oplevert, kan de Instelling na voorafgaande aparte toestemming hiervoor, overgaan tot het kennisnemen van de inhoud van communicatie of opgeslagen bestanden. Indien het onderzoek geen aanleiding geeft tot verdere maatregelen wordt de vastlegging vernietigd.

Nader onderzoek naar de beveiliging of integriteit van randapparatuur mag in afwijking hiervan door de ict-beheerder worden uitgevoerd op basis van concrete aanwijzingen, zonder aparte toestemming. De resultaten van dit onderzoek worden alleen gedeeld met de deelnemer met het doel de beveiliging of integriteit van de randapparatuur te verbeteren. Bij herhaling zal de procedure zoals hiervoor beschreven voor het gericht onderzoek worden gevolgd.

De deelnemer wordt zo spoedig mogelijk schriftelijk geïnformeerd door de directeur over de aanleiding, de uitvoering en het resultaat van het onderzoek. De deelnemer wordt in de gelegenheid gesteld uitleg te geven over de aangetroffen gegevens. Uitstel van het informeren mag alleen als informeren het onderzoek daadwerkelijk zou schaden.

Ict-beheerders verschaffen zich slechts toegang tot accounts of computers van de deelnemer als de deelnemer daarvoor zijn toestemming heeft gegeven. Toegang zonder deze toestemming is slechts toegestaan in dringende gevallen of bij een duidelijk vermoeden van schending van dit Reglement, zoals nader bepaald in dit reglement. De deelnemer zal in dat geval achteraf worden geïnformeerd.

### Rechten van de deelnemer met betrekking tot persoonsgegevens

Zie **“Privacy reglement voor deelnemers”**, bijlage 1.

### Consequenties van overtreding

Bij handelen in strijd met dit Reglement of algemeen geldende (wettelijke) regels, kan de Instelling afhankelijk van de aard en de ernst van de overtreding disciplinaire maatregelen treffen. Hieronder vallen een waarschuwing, berisping, een tijdelijke afsluiting of beperking van de faciliteiten (maximaal een jaar) en in extreme gevallen een beëindiging van de inschrijving als deelnemer.

Disciplinaire maatregelen (behalve een waarschuwing) kunnen niet worden getroffen enkel op basis van een langs geautomatiseerde weg uitgevoerde verwerking van persoonsgegevens, zoals een constatering van een automatisch filter of blokkade. Voorts worden geen disciplinaire maatregelen getroffen zonder dat de deelnemer gelegenheid heeft gekregen zijn zienswijze naar voren te brengen.

In afwijking van het voorgaande is het mogelijk dat de Instelling bij (geautomatiseerde) constatering van overlast een tijdelijke blokkade van de betreffende faciliteit invoert. Deze blokkade zal maximaal een week worden gehandhaafd of korter als de oorzaak naar tevredenheid van de ict-beheerder is weggenomen. Indien na een week geen verbetering is geconstateerd door de ict-beheerder, kan deze besluiten tot een langere blokkade. Bij herhaling van de oorzaak kunnen alsnog disciplinaire maatregelen worden genomen.

### Slotbepalingen

Dit Reglement kan door de Instelling worden herzien. Wijzigingen worden alleen bij het begin van een collegejaar doorgevoerd, behalve in dringende gevallen of wanneer de Instelling door omstandigheden van buitenaf gedwongen is tot een snellere invoering. Wijzigingen worden alleen ingevoerd nadat de Ondernemingsraad om voorafgaand advies is gevraagd. De Instelling zal feedback van deelnemers in overweging nemen alvorens de wijzigingen in te voeren. In gevallen waarin dit Reglement niet voorziet, beslist de Raad van Bestuur.

## Reglement Verantwoord Netwerkgebruik voor medewerkers

### Basis voor het reglement

Het gebruik van internet en ICT-middelen[[1]](#footnote-1) is voor (veel van) de medewerkers binnen [instelling] noodzakelijk om hun werk goed te kunnen doen. Aan het gebruik hiervan zijn risico’s verbonden die het stellen van gedragsregels noodzakelijk maken. Tegen de achtergrond van deze risico’s mag van de medewerkers verantwoord gebruik van internet en ICT worden verwacht.

Met dit Reglement wil de [Instelling], gevestigd te [adres Instelling], hierna te noemen de “Instelling” regels stellen omtrent het gewenst gebruik van deze bedrijfsmiddelen. Het streven daarbij is een goede balans aan te brengen tussen verantwoord en veilig ICT- en internetgebruik.

Afspraken in het kader van privacy worden in een apart reglement geregeld, het “**Privacy reglement voor medewerkers”,** zie bijlage 2**.**

Het gebruik van social media zoals Facebook, LinkedIn en Twitter wordt steeds belangrijker maar kan ook zijn weerslag hebben op de Instelling. Daarom wil de Instelling ook hier bepaalde regels aan stellen. Deze zijn opgenomen in het “**Protocol social media voor medewerkers en deelnemers”**, zie bijlage 3.

De Instelling is als werkgever bevoegd regels te stellen omtrent de uitvoering van het werk en de goede orde op de werkvloer, zo volgt uit de wet.

**Artikel 1. Uitgangspunten**

1.1. Het Reglement stelt regels ten aanzien van het gebruik van de bedrijfsmiddelen ICT en internet door medewerkers. Doel van deze regels is de goede orde te bepalen ten aanzien van:

* systeem- en netwerkbeveiliging, inclusief beveiliging tegen schade en mis-bruik;
* tegengaan van seksuele intimidatie, discriminatie en andere strafbare feiten;
* bescherming van privacy gevoelige informatie waaronder en persoonsgege-vens van de Instelling en haar medewerkers, en van deelnemers en ouders;
* bescherming van vertrouwelijke informatie van de Instelling en haar mede-werkers, en van deelnemers en ouders;
* bescherming van de intellectuele eigendomsrechten van de Instelling en derden waaronder het respecteren van de licentie-afspraken die van toepassing zijn binnen de Instelling;
* voorkomen van negatieve publiciteit;
* kosten- en capaciteitsbeheersing.

1.2. Beperkt privégebruik van internet en ICT-middelen is alleen toegestaan tijdens pauzes en/of voor zover het werk er niet onder lijdt.

1.3. Dit Reglement geldt voor een ieder die voor de Instelling werkzaam is, dus ook voor uitzendkrachten en tijdelijke medewerkers. Het Reglement geldt niet voor (gast)deelnemers; hiervoor is het aparte Deelnemersreglement opgesteld.

1.4. De Instelling streeft in het kader van handhaving van dit Reglement naar maatregelen die inzage in privacygevoelige informatie of persoonsgegevens van individuele medewerkers zo veel mogelijk beperken. Zij zal waar mogelijk slechts geautomatiseerd controleren of filteren zonder daarbij zichzelf of andere personen inzage te geven in gedrag van individuele personen.

**Artikel 2. Intellectueel eigendom en vertrouwelijke informatie**

2.1. De medewerker dient vertrouwelijke informatie, privacygevoelige informatie waaronder persoonsgegevens waar hij in het kader van het werk toegang tot heeft, strikt vertrouwelijk te behandelen en voldoende maatregelen te treffen om de vertrouwelijkheid te waarborgen.

2.2. De medewerker maakt geen inbreuk op de intellectuele eigendomsrechten van de Instelling en derden en respecteert licentieafspraken zoals die van toepassing zijn binnen de Instelling.

2.3. De zeggenschap over de informatie van de Instelling berust bij Instelling. De medewerker heeft geen zelfstandige zeggenschap over de informatie behalve als hem dat expliciet is toegekend door de Instelling.

2.4. De medewerker besteedt bijzondere aandacht aan het treffen van maatregelen zoals in dit Reglement genoemd, indien in het kader van het uitvoeren van de werkzaamheden de verwerking van vertrouwelijke informatie buiten de Instelling noodzakelijk is zoals via E-mail, in niet instellingsgebonden Cloud-toepassingen, op externe opslagmedia of eigen client-apparatuur (USB-apparaten, Tablets, etc.).
Indien de Instelling met betrekking tot het waarborgen van de vertrouwelijkheid voorschriften heeft opgesteld zal medewerker deze strikt naleven.

**Artikel 3. Gebruik van computer- en netwerkfaciliteiten**

3.1. Computer- en netwerkfaciliteiten worden beschikbaar gesteld aan de medewerker voor gebruik in het kader van zijn functie. Gebruik is derhalve verbonden aan taken die voortvloeien uit deze functie. Privégebruik van deze middelen is alleen toegestaan zoals bepaald in artikel 1.2.

3.2. De medewerker dient te allen tijde zorgvuldig om te gaan met aan hem persoonlijk toegekende inloggegevens en eventuele aanvullende authenticatiemiddelen (zoals smartcards en tokens). Persoonsgebonden wachtwoorden en aanvullende authenticatiemiddelen mogen niet worden gedeeld. Bij een vermoeden van misbruik van een wachtwoord kan de ict-beheerder per direct het betrokken account ontoegankelijk maken.

3.3. Het installeren van software op de computer- en netwerkfaciliteiten van de organisatie is niet toegestaan zonder aparte toestemming van de ict-beheerder. Ook het aansluiten van servers en actieve netwerkcomponenten (zoals access points en routers is niet toegestaan zonder toestemming van de ict-beheerder.

 De ict-beheerder kan aan de toestemming regels verbinden ter handhaving van dit reglement, zoals het moeten installeren van virusscanners en wachtwoord-beveiliging.

 Het aansluiten van eigen client-apparatuur (zoals, laptops, tablets en telefoons) is alleen toegestaan op de daarvoor beschikbaar gestelde (wireless) netwerkaansluitingen. De ict-beheerder kan aan de toegang tot deze aansluitingen regels verbinden ter handhaving van dit reglement, zoals het moeten installeren van virusscanners en wachtwoordbeveiliging.

3.4. Het opslaan van privébestanden of -informatie op systemen van de Instelling is toegestaan, mits dit niet leidt tot overbelasting van de opslagcapaciteit van deze systemen of een verstoring van de goede orde op de werkvloer. De Instelling is echter niet verplicht van dergelijke bestanden of informatie reservekopieën te maken of kopieën beschikbaar te stellen bij vervanging of reparatie van de betreffende systemen.

3.5. Het gebruik van computer- en netwerkfaciliteiten door de medewerker ten behoeve van nevenwerkzaamheden is uitsluitend toegestaan als en voor zover de Instelling hiervoor schriftelijk toestemming heeft verleend.

**Artikel 4. Gebruik van e-mail en andere ICT-communicatiemid-delen**

4.1. Het e-mailsysteem en de bijbehorende mailbox en het e-mailadres wordt aan de medewerker voor gebruik in het kader van zijn functie beschikbaar gesteld. Gebruik is derhalve verbonden aan taken die voortvloeien uit deze functie.

4.2. Privégebruik van deze middelen is alleen toegestaan zoals bepaald in artikel 1.2.

4.3. Verboden bij elk gebruik (privé of niet) van ICT-communicatiemiddelen is echter:

* het verzenden van berichten met een pornografische, racistische, discriminerende, bedreigende, beledigende of aanstootgevende inhoud;
* het verzenden van berichten met een (seksueel) intimiderende inhoud;
* het verzenden van berichten die (kunnen) aanzetten tot discriminatie, haat en/of geweld;
* het versturen van ongevraagde berichten aan grote aantallen ontvangers, kettingbrieven te versturen of kwaadaardige software zoals virussen, Trojaanse paarden of spyware te versturen.

4.4. De medewerker gebruikt voor privémail bij voorkeur niet het door de Instelling verstrekte e-mail adres, binnen de grenzen van artikel 1.2. De organisatie zal de toegang tot andere e-maildiensten niet blokkeren of specifiek monitoren.

4.5. In geval van ziekte, onverwacht langdurige afwezigheid of grove nalatigheid van de medewerker, doch uitsluitend als dit een zwaarwegende reden van bedrijfsbelang tot toegang oplevert, is de Instelling gerechtigd een vervanger of leidinggevende toegang tot de bestanden of mailbox van de medewerker te verschaffen doch uitsluitend nadat hiertoe expliciet toestemming van de directeur van de medewerker is verkregen en dit door de directeur kenbaar is gemaakt aan de betreffende medewerker. Deze mag zich echter geen toegang verschaffen tot als privé gemarkeerde mappen, als privé herkenbare mails, of mails verzonden naar dan wel afkomstig van een vertrouwenspersoon of bedrijfsarts. Indien de medewerker geen dergelijke markeringen heeft aangebracht, kan de Instelling door inschakeling van een vertrouwenspersoon de betreffende informatie van de medewerker controleren om zo privéinformatie te herkennen en te separeren alvorens de vervanger of leidinggevende toegang krijgt.

 Dit Artikel 4.5 is ter goedkeuring voorgelegd aan de OR (WOR, artikel 27, lid K).

4.6. E-mailberichten van leden van het medezeggenschapsorgaan onderling, van bedrijfsartsen en van een ieder die zich op grond van de wet op vertrouwelijkheid mag beroepen, worden niet gecontroleerd. Dit geldt niet voor geautomatiseerde controle op de veiligheid van het e-mailverkeer en netwerk.

**Artikel 5 Gebruik van internet**

5.1. De toegang tot internet en bijbehorende faciliteiten worden aan de medewerker voor gebruik in het kader van zijn functie beschikbaar gesteld. Gebruik is derhalve verbonden aan taken die voortvloeien uit deze functie.

5.2. Privégebruik van deze middelen is alleen toegestaan zoals bepaald in artikel 1.2.

5.3. Verboden bij elk gebruik (privé of niet) is echter:

* sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten;
* filesharing- of streamingdiensten (zoals internetradio of Uitzendinggemist) te gebruiken wanneer dit overmatig veel dataverkeer genereert, zodanig dat het de beschikbaarheid van de faciliteiten in gevaar kan brengen;
* films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van enige illegale bron of wanneer de medewerker daadwerkelijk weet dat dit in strijd met auteursrechten is;
* films, muziek, software en overig auteursrechtelijk beschermd materiaal te verspreiden (uploaden) naar derden zonder toestemming van de rechthebbenden.

**Artikel 6. Gebruik van sociale media**

6.1. [Instelling] ondersteunt de open dialoog en de uitwisseling van ideeën en het delen van kennis van de medewerker met vakgenoten en derden via sociale media (zoals Facebook, Youtube, MSN, Skype, Omegle, Twitter of Linkedin). Indien dit werkgerelateerde onderwerpen betreft, dient de medewerker altijd de Instelling en zijn functie te vermelden, alsmede een disclaimer waarin staat dat het een persoonlijk standpunt betreft, dat niet overeen hoeft te komen met dat van de Instelling.

6.2. Medewerker zal geen deelnemers toevoegen als ‘vrienden’ of contacten op dergelijke sociale media, tenzij hij hiertoe een apart profiel hanteert dat duidelijk aan de Instelling gelinkt is en waar de Instelling eisen ten aanzien van presentatie, inhoud en functioneren aan kan stellen.

6.3. Bestuurders, managers, leidinggevenden en anderen die namens [instelling] beleid of strategie uitdragen hebben een bijzondere verantwoordelijkheid bij het gebruik van sociale media, ook als de inhoud niet direct verband houdt met hun werk. Op grond van hun positie moeten zij nagaan of zij op persoonlijke titel kunnen publiceren. Zij zijn zich ervan bewust dat medewerkers lezen wat zij schrijven.

6.4. Dit artikel geldt ook indien medewerkers vanaf privécomputers of -internetaansluitingen deelnemen aan sociale media, doch uitsluitend voor zover het gaat om deelname die het werk kan raken.

6.5. Wanneer medewerker een sociale-media-account opzet dat direct werk gerelateerd is, terwijl het op naam van medewerker persoonlijk is gesteld, zullen medewerker en de Instelling bij beëindiging van het dienstverband een passende oplossing zoeken voor het overdragen van dit profiel of de informatie en contacten daarop.

**Artikel 7. Monitoring en controle**

7.1. Controle van gebruik van de ICT-faciliteiten en internetgebruik vindt slechts plaats in het kader van handhaving van de regels uit dit reglement voor de doelen genoemd in Artikel 1. Verboden gebruik van de bedrijfsmiddelen wordt zo veel mogelijk langs technische weg onmogelijk gemaakt.

7.2. Ten behoeve van controle op de naleving van de regels worden gegevens geautomatiseerd verzameld (gelogd). Deze gegevens zijn alleen toegankelijk voor de direct verantwoordelijke systeembeheerders en worden alleen in geanonimiseerde vorm aan overige beheerders en andere verantwoordelijken beschikbaar gesteld. Deze kunnen tot nadere technische maatregelen besluiten.

7.3. Bij vermoedens van overtreding van de regels kan controle worden uitgevoerd op het niveau van individuele verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen vindt controle op de inhoud plaats.

7.4. De Instelling houdt zich bij het controleren op het niveau van verkeersgegevens of persoonsgegevens onverkort aan de Wet bescherming persoonsgegevens en andere relevante wet- en regelgeving. In het bijzonder beveiligt de Instelling de bij controle vastgelegde gegevens tegen ongeautoriseerde toegang en zijn personen met toegang daartoe contractueel verplicht tot geheimhouding.

7.5. Enkele specifieke maatregelen ter controle die de Instelling kan voeren, zijn:

* controle ter voorkoming van negatieve publiciteit en seksuele intimidatie en de controle in het kader van systeem- en netwerkbeveiliging vindt plaats op basis van filtering van de inhoud op trefwoorden. Verdachte berichten worden automatisch teruggestuurd naar de afzender;
* controle in het kader van kosten- en capaciteitsbeheersing wordt beperkt tot het op basis van verkeersgegevens nagaan van de bronnen van kosten of capaciteitsvraag (zoals de adressen van internetradio en videosites). Als deze websites tot grote kosten of overlast leiden, worden zij geblokkeerd of afgeknepen, zonder daarbij de vertrouwelijkheid van de inhoud van de communicatie te schenden;
* controle op het gebruik van beeldmateriaal vindt plaats op basis van klachten of meldingen van derden, of steekproefsgewijs bij beeldmateriaal dat openbaar beschikbaar is.

**Artikel 8. Procedure bij gericht onderzoek**

8.1. Van gericht onderzoek is sprake wanneer verkeersgegevens of andere persoonsgegevens betreffende een specifieke medewerker worden vastgelegd in het kader van een onderzoek naar aanleiding van een zwaarwegend vermoeden van een overtreding van dit Reglement door die medewerker.

8.2. Gericht onderzoek vindt uitsluitend plaats na schriftelijke opdracht van de directeur van de betreffende school. De Raad van Bestuur ontvangt een afschrift van deze opdracht en een vastlegging van de resultaten van het onderzoek. Indien het onderzoek geen aanleiding geeft tot verdere maatregelen wordt de vastlegging vernietigd.

8.3. In afwijking van het vorige lid vindt gericht onderzoek naar de beveiliging of integriteit van randapparatuur plaats door de ict-beheerder op basis van concrete aanwijzingen. Aparte toestemming van de in lid 2 bedoelde instantie is niet nodig. De resultaten van dit onderzoek worden alleen gedeeld met de medewerker met het doel de beveiliging of integriteit van de randapparatuur te verbeteren. Bij herhaling zal de procedure uit lid 2 worden gevolgd.

8.4. Gericht onderzoek beperkt zich in eerste instantie tot verkeersgegevens van het gebruik van de faciliteiten. Als gericht onderzoek nader bewijs oplevert, kan de Instelling overgaan tot het kennisnemen van de inhoud van communicatie of opgeslagen bestanden. Dit vereist schriftelijke toestemming van de Raad van Bestuur, welke toestemming de redenen zal noemen waarom deze wordt verleend. De Instelling zal zich maximaal inspannen de identiteit van de personen die deze kennisneming uitvoeren, geheim te houden. De vastlegging wordt onder naam van de directeur gedaan.

8.5. Enkele specifieke persoonsgebonden maatregelen ter controle die de Instelling kan voeren, zijn:

* controle op het uitlekken van vertrouwelijke informatie vindt plaats op basis van steekproefsgewijze controle op trefwoorden. Verdachte berichten worden apart gezet voor nader onderzoek in overleg met het bestuur;
* controle op overtreding van het verbod uit Artikel 4 lid 3 vindt plaats door twee personen op klacht [of steekproefsgewijs] e-mailberichten te openen en de inhoud te raadplegen. Deze personen zijn gebonden aan geheimhouding over de inhoud;

8.6. De medewerker wordt zo spoedig mogelijk schriftelijk geïnformeerd door de directeur over de aanleiding, de uitvoering en het resultaat van het onderzoek. De medewerker wordt in de gelegenheid gesteld uitleg te geven over de aangetroffen gegevens. Uitstel van het informeren mag alleen als informeren het onderzoek daadwerkelijk zou kunnen schaden.

8.7. Systeembeheerders verschaffen zich slechts toegang tot accounts of computers van medewerkers als de medewerker daarvoor zijn toestemming heeft gegeven. Toegang zonder deze toestemming is slechts toegestaan in dringende gevallen of bij een duidelijk vermoeden van schending van dit Reglement, zoals nader bepaald in dit Artikel. De medewerker zal in dat geval achteraf worden geïnformeerd.

**Artikel 9. Rechten van de medewerker mbt persoonsgegevens**

VERVALLEN EN VERVANGEN DOOR : Privacy reglement voor medewerkers, zie bijlage 1

**Artikel 10. Consequenties van overtreding**

10.1. Bij handelen in strijd met dit Reglement of de algemeen geldende wettelijke regels, kan het bestuur afhankelijk van de aard en de ernst van de overtreding disciplinaire maatregelen treffen. Hieronder vallen een waarschuwing, berisping, overplaatsing, schorsing en beëindiging van de arbeidsovereenkomst. Daarnaast kan het bestuur besluiten tot een al dan niet tijdelijke beperking in de toegang tot bepaalde ICT-faciliteiten.

10.2. Disciplinaire maatregelen (behalve een waarschuwing) kunnen niet worden getroffen enkel op basis van een langs geautomatiseerde uitgevoerde verwerking van persoonsgegevens, zoals een constatering van een automatisch filter of blokkade. Voorts worden geen disciplinaire maatregelen getroffen zonder dat de medewerker gelegenheid heeft gekregen zijn zienswijze naar voren te brengen.

10.3. Aanvullend op voorgaande is het mogelijk dat de Instelling bij (geautomatiseerde) constatering van overlast een tijdelijke blokkade van de betreffende faciliteit invoert. Deze blokkade zal zolang worden gehandhaafd tot aangetoond is dat de oorzaak is weggenomen. Bij herhaling van de oorzaak kunnen disciplinaire maatregelen worden genomen.

**Artikel 11. Slotbepaling**

11.1. Dit Reglement wordt jaarlijks geëvalueerd door de Raad van Bestuur van [instelling]. De Instelling betrekt medezeggenschapsorganen bij de evaluatie/Medezeggenschapsorganen kunnen ook zelfstandig het advies nemen het Reglement te evalueren. De eerstkomende evaluatie vindt plaats in [MAAND JAAR].

11.2. [Instelling] kan dit Reglement met instemming van het medezeggenschapsorgaan wijzigen als de omstandigheden daar aanleiding toe geven. Voorgenomen wijzigingen worden voorafgaand aan de invoering aan de medewerkers bekend gemaakt. De Raad van Bestuur zal feedback van medewerkers in overweging nemen alvorens de wijzigingen in te voeren.

11.3. In gevallen waarin dit Reglement niet voorziet, beslist het College van Bestuur.

**Bijlage 1:**

**Privacy reglement voor deelnemers**

**1. Aanhef**

Dit reglement is voor [Instelling].

**2. Definities**

Persoonsgegevens:: Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;

Verwerking van persoonsgegevens: Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;

Bijzonder persoonsgegeven: Een persoonsgegeven dat iets zegt over iemand zijn godsdienst, levensovertuiging, ras, politieke gezindheid of zijn gezondheid;

Betrokkene: Degene op wie een persoonsgegeven betrekking heeft al dan niet vertegenwoordigd door diens wettelijk vertegenwoordiger. In dit reglement gaat het om de leerlingen;

Wettelijk vertegenwoordiger: Indien de betrokkene de leeftijd van zestien jaren nog niet heeft bereikt, wordt de betrokkene vertegenwoordigd door zijn wettelijk vertegenwoordiger. Meestal zal dit een ouder zijn maar het kan hier ook gaan om een voogd;

Verantwoordelijke: De verantwoordelijke stelt vast welke persoonsgegevens er verwerkt worden én wat het doel is van die verwerking. Dat wil zeggen de (openbare of privaatrechtelijke) rechtspersoon waar [instelling] onder valt: het bevoegd gezag. Wanneer er in dit regelement gesproken wordt over de Verantwoordelijke dan wordt daarmee het bevoegd gezag van [instelling] bedoeld;

Bewerker: Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;

Derde: Ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken;

[Instelling]: De verantwoordelijke onderwijsinstelling / het bevoegd gezag.

Wbp: Wet Bescherming Persoonsgegevens;

Vrijstellingsbesluit Wbp: Besluit van 7 mei 2001, (Staatsblad 2001, 250), houdende aanwijzing van verwerkingen van persoonsgegevens die zijn vrijgesteld van de melding bedoeld in artikel 27 van de Wet bescherming persoonsgegevens.

**3. Reikwijdte en doelstelling**

3.1. Dit reglement stelt regels over de verwerking van persoonsgegevens van studenten van [instelling]

3.2. Dit reglement is van toepassing op alle persoonsgegevens van de betrokkene die door [instelling] worden verwerkt. Dit reglement heeft tot doel:

1. de persoonlijke levenssfeer van de betrokkenen te beschermen tegen verkeerd en onbedoeld gebruik van de persoonsgegevens;
2. vast te stellen welke persoonsgegevens worden verwerkt en met welk doel dit gebeurt;
3. de zorgvuldige verwerking van persoonsgegevens te waarborgen;

d. de rechten van betrokkene te waarborgen.

**4. Doelen van de verwerking van persoonsgegevens**

Bij de verwerking van persoonsgegevens houdt [instelling] zich aan relevante wetgeving waaronder de Wet bescherming persoonsgegevens.

*Doelen*

De verwerking van persoonsgegevens vindt plaatst voor:

1. de organisatie of het geven van het onderwijs, de begeleiding van leerlingen, deelnemers of studenten, dan wel het geven van studieadviezen;
2. het verstrekken of ter beschikking stellen van leermiddelen
3. het bekend maken van informatie over de organisatie en leermiddelen als bedoeld, onder a en b, alsmede informatie over de leerlingen, deelnemers of studenten, bedoeld in het eerste lid, op de eigen website;
4. het bekendmaken van de activiteiten van de instelling of het instituut op de eigen website;
5. het berekenen, vastleggen en innen van inschrijvingsgelden, [instelling]- en lesgelden en bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten, waaronder begrepen het in handen van derden stellen van vorderingen;
6. het behandelen van geschillen en het doen uitoefenen van accountantscontrole;
7. het onderhouden van contacten met de oud-leerlingen, oud-deelnemers of oud-studenten van de verantwoordelijke;
8. de uitvoering of toepassing van een andere wet.

**5. Vrijstelling meldingsplicht**

De in artikel 4 genoemde gegevensverwerkingen vallen onder het vrijstellingsbesluit Wbp en hoeven niet te worden aangemeld bij de AP.

**6. Doelbinding**

Persoonsgegevens worden uitsluitend gebruikt voor zover dat gebruik verenigbaar is met de omschreven doelen van de verwerking. De [instelling] verwerkt niet meer gegevens dan noodzakelijk is om die vastgestelde doelen te bereiken.

**7. Soorten gegevens**

De door [instelling] gebruikte categorieën van persoonsgegevens worden in bijlage 1 opgesomd.

**8. Grondslag verwerking**

Verwerking van persoonsgegevens gebeurt alleen op grond van:

1. Toestemming: in het geval de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend.
2. Overeenkomst: in het geval de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst.

1. Wettelijke verplichting: in het geval de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de [instelling] onderworpen is.
2. Vitaal belang: (bescherming van betrokkene): het verwerken van persoonsgegevens is noodzakelijk om een ernstige bedreiging te beperken/voorkomen van de gezondheid van de betrokkene.
3. Publiekrechtelijke taak: in het geval de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt
4. Gerechtvaardigd belang (belangenafweging): de gegevensverwerking is noodzakelijk voor de behartiging van een gerechtvaardigd belang van de verantwoordelijke, waarbij het belang van het verwerken van de gegevens zwaarder weegt dan het privacybelang van de betrokkene.

**9. Bewaartermijnen**

[Instelling] bewaart de gegevens niet langer dan dat zij noodzakelijk zijn voor het vervullen van het doel waarvoor zij zijn verkregen, tenzij er een andere wettelijke verplichting is die het langer bewaren van de gegevens verplicht stelt.

**10. Toegang**

ROC West-Brabant verleent slecht toegang tot de in de administratie en systemen van de [instelling] opgenomen persoonsgegevens aan:

1. de bewerker en de derde die onder rechtstreeks gezag van [instelling] staat;
2. de bewerker die gemachtigd is om persoonsgegevens te verwerken;’
3. derden die op grond van de wet toegang moet worden verleend, waarbij alleen toegang wordt verleend aan de gegevens waartoe volgens de wet toegang toe moet worden gegeven.

**11. Beveiliging en geheimhouding**

a. [Instelling] neemt passende technische en organisatorische beveiligingsmaatregelen om te voorkomen dat de persoonsgegevens worden beschadigd, verloren gaan of onrechtmatig worden verwerkt. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

b. [Instelling] zorgt dat medewerkers niet meer inzage of toegang hebben tot de persoonsgegevens dan zij strikt noodzakelijk nodig hebben voor de goede uitoefening van hun werk.

c. Bij de beveiligingsmaatregelen wordt rekening gehouden met de stand van de techniek en de kosten van de tenuitvoerlegging. Daarbij houdt de [instelling] rekening met de concrete risico’s die van toepassing kunnen zijn op de verwerkte persoonsgegevens.

d. Iedereen die betrokken is bij de uitvoering van dit reglement, en daarbij de beschikking krijgt over persoonsgegevens die vertrouwelijk zijn of geheim moeten worden gehouden (zoals bijvoorbeeld zorggegevens), en voor wie niet reeds uit hoofde van beroep, functie of wettelijk voorschrift een geheimhoudingsplicht geldt, is verplicht tot geheimhouding van die persoonsgegevens daarvan.

**12. Verstrekken gegevens aan derden**

Wanneer daartoe een wettelijke plicht bestaat kan [instelling] de persoonsgegevens verstrekken aan derden. Het verstrekken van persoonsgegevens aan derden kan ook plaatst vinden na toestemming van de betrokkene.

**13. Sociale media**

Voor het gebruik van persoonsgegevens in sociale media, zijn aparte afspraken gemaakt in het ‘sociale-mediaprotocol’ van [instelling].

**14. Rechten betrokkenen**

14.1. De Wbp geeft de betrokkene een aantal rechten. [Instelling] erkent deze rechten en handelt in overeenstemming met deze rechten.

14.1.1 *Inzage*

Elke betrokkene heeft recht op inzage van de door [instelling] verwerkte persoonsgegevens die op hem/haar betrekking hebben. De [instelling] mag voor het inwilligen van dit verzoek een kostprijs verbinden van maximaal € 5,-. Wanneer het verzoek wordt afgewezen dan worden er geen kosten in rekening gebracht. [Instelling] kan vragen om een geldig identiteitsbewijs ter verificatie van de identiteit van de verzoeker.

14.1.2. *Verbetering, aanvulling, verwijdering en afscherming*

Betrokkene kan een verzoek doen tot verbetering, aanvulling, verwijdering of afscherming van zijn persoonsgegevens, tenzij dit onmogelijk blijkt of een onredelijke inspanning zou vergen.

14.1.3. *Verzet*

Voor zover de [instelling] persoonsgegevens gebruikt op de grond van artikel 8 onder e en f, dan kan de betrokkene zich verzetten tegen verwerking van persoonsgegevens op basis van diens persoonlijke omstandigheden.

14.2. *Termijn*

 [Instelling] dient binnen een termijn van 4 weken na ontvangst van een verzoek hieraan schriftelijk gehoor te geven dan wel deze schriftelijk, gemotiveerd af te wijzen. [Instelling] kan de betrokkene laten weten dat er meer tijd nodig en deze termijn verlengen met maximaal 4 weken.

14.3 *Uitvoeren verzoek*

Indien het verzoek van de betrokkene wordt gehonoreerd, draagt de[instelling] zorg voor het zo spoedig mogelijk doorvoeren van de verzochte wijzigingen.

14.4 *Intrekken toestemming*

Voor zover voor de verwerking van persoonsgegevens voorafgaande toestemming vereist is, kan deze toestemming ten allen tijden door de wettelijk vertegenwoordiger worden ingetrokken.

**15. Transparantie**

15.1. De [instelling] informeert de betrokkene over de verwerking van zijn persoonsgegevens. Indien het type verwerking dat vraagt, informeert de [instelling] iedere betrokkene apart over de details van die verwerking.

15.2. De [instelling] informeert de betrokkene – op hoofdlijnen – ook over de afspraken die gemaakt zijn met derden en bewerkers die persoonsgegevens van de betrokkene ontvangen.

**16. Klachten**

16.1. Wanneer u van mening bent dat het doen of nalaten van de [instelling] niet in overeenstemming is met de Wbp of zoals dat is uitgewerkt in dit reglement is, dan dient u zich te wenden tot [INVULLEN] van [instelling].

16.2. Overeenkomstig de Wpb kan de betrokkene zich eveneens wenden tot de rechter of het College bescherming persoonsgegevens.

**17. Onvoorziene situatie**

Indien er zich een situatie voordoet die niet beschreven is in dit reglement dan neemt de verantwoordelijke de benodigde maatregelen.

**18. Wijzigingen reglement**

Dit reglement wordt na instemming van de (OR vastgesteld door de verantwoordelijke. De verantwoordelijke maakt dit reglement openbaar via [INVULLEN].

De verantwoordelijke heeft het recht dit reglement, na instemming van de (G)MR te wijzigingen.

**19. Slotbepaling**

Dit reglement wordt aangehaald als het “privacyreglement deelnemers ” van [instelling] en treed in werking op [DATUM].

**BIJLAGE 1.1: Overzicht van categorieën gebruikte persoonsgegevens**

Omschrijving en opsomming categorieën Persoonsgegevens die gebruikt worden:

**Bijvoorbeeld:**

1. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie bedoelde gegevens van de betrokkene;
2. het persoonsgebonden nummer (BSN);
3. nationaliteit;
4. gegevens als bedoeld onder a, van de wettelijk vertegenwoordiger of verzorger van de leerling;
5. gegevens betreffende de gezondheid of het welzijn van de leerling voor zover die noodzakelijk zijn voor de ondersteuning;
6. gegevens betreffende de godsdienst of levensovertuiging van de leerling, voor zover die noodzakelijk zijn voor de [instelling], het onderwijs of de te geven ondersteuning;
7. gegevens betreffende de aard en het verloop van het onderwijs en ondersteuning, alsmede de behaalde studieresultaten;
8. [instelling] gegevens (waaronder naam [instelling], naam zorgcoördinator/mentor/ intern begeleider, klas/groep waarin de leerling zit, tijdstip van inschrijving bij deze [instelling], naam van de indiener van de aanmelding bij het samenwerkingsverband, [instelling]loopbaan en rapportage vanuit primair en voortgezet onderwijs);
9. aanleiding voor de aanmelding bij het samenwerkingsverband, relevante screenings- en onderzoeksgegevens en omschrijving van de problematiek die aan de orde is;
10. activiteiten die door de [instelling] zijn ondernomen rond de betreffende leerling, alsmede de resultaten hiervan;
11. bestaande of (relevante) afgesloten hulpverleningscontacten en de namen van contactpersonen;
12. relevante persoonsgegevens die door externe partijen worden verstrekt met betrekking tot de aangemelde problematiek van de betreffende leerling;
13. relevante financiële gegevens over bijvoorbeeld [instelling]geld;
14. etc.

**Bijlage 2:**

**Privacy reglement voor medewerkers**

**1. Aanhef**

Dit reglement is voor [Instelling].

**2. Definities**

Personeel: Bij of voor het bevoegd gezag werkzame personen;

Persoonsgegevens:: Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;

Verwerking van persoonsgegevens: Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;

Bijzonder persoonsgegeven: Een persoonsgegeven dat iets zegt over iemand zijn godsdienst, levensovertuiging, ras, politieke gezindheid of zijn gezondheid;

Betrokkene: Degene op wie een persoonsgegeven betrekking heeft al dan niet vertegenwoordigd door diens wettelijk vertegenwoordiger. In dit reglement gaat het om de leerlingen;

Burgerservicenummer: Het volgens de Wet algemene bepalingen Burgerservicenummer aan een natuurlijke persoon toegekend uniek persoonsnummer;

Bestand: Elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen;

Verantwoordelijke: Het bevoegd gezag van [instelling];

Bewerker: Degene die op basis van een overeenkomst ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;

Gebruiker: Degene in de zin van artikel 6 die gerechtigd is kennis te nemen van bepaalde gegevens in een persoonsregistratie;

Derde: Ieder niet zijnde de betrokkene, de verantwoordelijke, de bewerker; degene(n) die onder gezag van de verantwoordelijke of de bewerker gemachtigd is (zijn) om persoonsgegevens te verwerken;

Ontvanger: Degene aan wie de persoonsgegevens worden verstrekt;

Bevoegd gezag: De Raad van Bestuur van [instelling].

Toestemming van betrokkene: Elke vrije, specifieke en op informatie berustende wilsuiting waarmee betrokkene aanvaardt dat de hem / haar betreffende persoonsgegevens worden verwerkt;

Wbp: Wet Bescherming Persoonsgegevens;

Vrijstellingsbesluit Wbp: Besluit van 7 mei 2001, (Staatsblad 2001, 250), houdende aanwijzing van verwerkingen van persoonsgegevens die zijn vrijgesteld van de melding bedoeld in artikel 27 van de Wet bescherming persoonsgegevens.

# Reikwijdte en doelstelling van het reglement

* 1. Dit reglement is van toepassing op alle persoonsgegevens betreffende het personeel die door of namens het bevoegd gezag worden verwerkt;
	2. Dit reglement heeft tot doel:
1. de persoonlijke levenssfeer van personeel van wie persoonsgegevens worden verwerkt te beschermen tegen misbruik van die gegevens en tegen het verwerken van onjuiste gegevens;
2. te voorkomen dat persoonsgegevens worden verwerkt voor een ander doel dan het doel waarvoor ze verzameld zijn;
3. de rechten van de betrokkenen te waarborgen.

# Doel en verwerking van de persoonsgegevens

* 1. Slechts die persoonsgegevens worden verwerkt, die rechtmatig verkregen zijn.
	2. Verwerking van de gegevens mag alleen geschieden voor de in lid 5 van deze bepaling genoemde categorieën van verwerking.
	3. De verwerking van de gegevens moet in overeenstemming zijn met het doel, waarvoor de verwerking is aangelegd. De doeleinden verschillen per categorie en zijn omschreven in de bij dit reglement behorende bijlagen.
	4. Geen andere gegevens mogen worden verwerkt dan de gegevens genoemd in de bij dit reglement behorende bijlagen.
	5. De categorieën van verwerking zijn:
		1. sollicitanten (bijlage 1);
		2. personeelsadministratie (bijlage 2);
		3. salarisadministratie (bijlage 3);
		4. uitkering bij ontslag (bijlage 4);
		5. pensioen en vervroegde uittreding (bijlage 5)

**5. Het beheer van (de verwerking van) persoonsgegevens**

Persoonsgegevens worden op naam van het personeelslid verzameld. De verzameling van persoonsgegevens van het personeelslid vormt het dossier.

**6. Verstrekking van gegevens**

De persoonsgegevens worden slechts verstrekt aan:

1. degenen, waaronder begrepen derden, die leiding geven aan of belast zijn met de verwerking van persoonsgegevens van personeel of die daarbij noodzakelijk zijn betrokken;
2. anderen, in de gevallen bedoeld in artikel 8 onder a, c en d, of artikel 9 (verenigbaar gebruik), derde lid, van de Wbp;
3. anderen, in de gevallen bedoeld in artikel 8 onder e en f, van de Wbp, voor zover het slechts gegevens betreft als bedoeld in artikel 3 van dit reglement, en nadat het voornemen daartoe aan betrokkene is medegedeeld en deze gedurende een redelijke termijn in de gelegenheid is geweest het recht als bedoeld in artikel 40 of 41 van de Wbp uit te oefenen.
4. vakbonden, voor zover het slechts gegevens betreft als bedoeld in artikel 3 van dit reglement, en nadat het voornemen daartoe aan betrokkene is medegedeeld en deze gedurende een redelijke termijn in de gelegenheid is geweest het recht als bedoeld in artikel 40 of 41 van de Wbp uit te oefenen.
5. vereniging van oud-personeelsleden.

**7. Toegang tot persoonsgegevens**

* 1. Behoudens daartoe strekkende wettelijke voorschriften in wet- en regelgeving hebben slechts toegang tot de persoonsgegevens:
1. degenen, waaronder begrepen derden, die zijn belast met of leiding geven aan de activiteiten die in verband staan met de verwerking van de gegevens of die daarbij noodzakelijk zijn betrokken;
2. anderen, in gevallen als bedoeld in artikel 8 onder a, c en d, en artikel 9 derde lid van de Wbp.

7.2 bijgevoegd als bijlage 6 bij dit reglement. Dit bestand kan worden geraadpleegd via de portal.

##### 8. Beveiliging en geheimhouding

8.1 De verantwoordelijke draagt zorg voor passende technische en organisatorische maatregelen ter voorkoming van verlies of onrechtmatige verwerking van persoonsgegevens. Deze maatregelen garanderen, rekening houdend met de stand der techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau, gelet op de risico’s die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

8.2 Indien sprake is van elektronische verwerking van persoonsgegevens zal de beheerder via een coderingsbeveiliging de verschillende functionarissen, als bedoeld in artikel 6, toegang geven tot bepaalde gedeelten van de persoonsgegevens of tot alle persoonsgegevens al naar gelang hun werkzaamheden dit vereisen.

8.3 Een ieder die betrokken is bij de uitvoering van dit reglement en daarbij de beschikking krijgt over persoonsgegevens waarvan hij het vertrouwelijke karakter kent of redelijkerwijs kan vermoeden en voor wie niet reeds uit hoofde van beroep, functie of wettelijk voorschrift ter zake van de persoonsgegevens een geheimhoudingsplicht geldt, is verplicht tot geheimhouding daarvan. Dit geldt niet indien enig wettelijk voorschrift hem tot bekendmaking verplicht of uit zijn taak bij de uitvoering van dit reglement de noodzaak tot bekendmaking voortvloeit.

**9. Informatieplicht**

* 1. De verantwoordelijke informeert betrokkene over het verwerken van diens persoonsgegevens, voorafgaand aan de verzameling van de persoonsgegevens of, indien de gegevens van derden afkomstig zijn, voorafgaand aan het moment van vastlegging.
	2. De verantwoordelijke informeert betrokkene over de persoonsgegevens die worden verwerkt, met welk doel dat gebeurt en aan wie de gegevens worden verstrekt.

###### 10. Rechten betrokkene(n): inzage, correctie, verzet

 9.1 Elke betrokkene heeft het recht op inzage. Aan een verzoek om inzage kunnen kosten worden verbonden.

* 1. Indien de verantwoordelijke twijfelt aan de identiteit van de verzoeker, vraagt hij zo spoedig mogelijk aan de verzoeker schriftelijk nadere gegevens inzake zijn identiteit te verstrekken of een geldig identiteitsbewijs te overleggen. Door dit verzoek wordt de termijn opgeschort tot het tijdstip dat het gevraagde bewijs is geleverd.
	2. Een verzoek om inzage dient te worden gedaan aan de verantwoordelijke, die binnen vier weken na ontvangst van dit verzoek hierop schriftelijk reageert.
	3. Indien de betrokkene de verantwoordelijke verzoekt tot correctie omdat bepaalde opgenomen gegeven onjuist c.q. onvolledig zouden zijn, dan wel gezien de doelstelling van het systeem niet ter zake doen, dan wel strijdig zijn met dit reglement, neemt de verantwoordelijke binnen vier weken nadat betrokkene dit verzoek heeft ingediend, hierover een beslissing.

* 1. De verantwoordelijke draagt zorg dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.
	2. Wanneer de verwerking van persoonsgegevens plaatsvindt op de grondslag dat die verwerking
	a. noodzakelijk is voor de goede vervulling van een door de verantwoordelijke verrichte publiekrechtelijke taak, of

b. noodzakelijk is voor een gerechtvaardigd belang van de verantwoordelijke of een derde,
kan betrokkene schriftelijk verzet aantekenen tegen de verwerking van de gegevens, op basis van zijn bijzondere persoonlijke omstandigheden.

De verantwoordelijke dient binnen vier weken na ontvangst van het verzet te beoordelen of het verzet terecht is. Is dat het geval, dan dient de verwerking van persoonsgegevens onmiddellijk te worden beëindigd.

* 1. Een beslissing op een verzoek om inzage, een beslissing als vermeld in lid 4 en de beoordeling als vermeld in lid 6 van deze bepaling zijn besluiten in de zin van de Algemene Wet Bestuursrecht.
	2. Wanneer de verwerking van persoonsgegevens plaatsvindt op de grondslag dat die verwerking geschiedt voor direct marketingdoeleinden, kan betrokkene eveneens schriftelijk verzet aantekenen tegen de verwerking van de gegevens. Indien betrokkene van dit recht gebruik maakt, dient de verwerking van persoonsgegevens voor dit doel onmiddellijk te worden beëindigd.

**11. Bewaartermijnen**

Hierbij onderscheiden we:

1. Administratie personeel / salaris: de persoonsgegevens worden verwijderd uiterlijk twee jaren nadat het dienstverband of de werkzaamheden van betrokkene ten behoeve van de verantwoordelijke zijn beëindigd, tenzij de persoonsgegevens noodzakelijk zijn ter voldoening aan een wettelijke bewaarplicht.
2. Administratie sollicitanten: de persoonsgegevens worden verwijderd op een daartoe strekkend verzoek van betrokkene en in ieder geval uiterlijk vier weken nadat de sollicitatieprocedure is geëindigd, tenzij de persoonsgegevens met toestemming van betrokkene gedurende een jaar na beëindiging van de sollicitatieprocedure worden bewaard.

**12 Oud-personeel**

12.1 De verantwoordelijke kan besluiten over te gaan tot het instellen van een verwerking van persoonsgegevens betreffende oud-personeelsleden

12.2 De verwerking geschiedt slechts voor:

 a. het onderhouden van contacten met oud-personeelsleden;

 b. het verzenden van informatie aan oud-personeelsleden;

 c. het berekenen, vastleggen en innen van bijdragen en giften, waaronder begrepen het in handen van derden stellen van vorderingen, alsmede andere activiteiten van intern beheer;
d. het behandelen van geschillen en het doen uitoefenen van accountantscontrole.

12.3 Geen andere persoonsgegevens worden verwerkt dan:

a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens, alsmede bankrekeningnummer van de betrokkene;

b. gegevens betreffende de functie waarin en de periode gedurende welke de het oud-personeelslid voor de verantwoordelijke werkzaam is geweest;

c. gegevens met het oog op het berekenen, vastleggen en innen van bijdragen en giften.

d. een administratiecode dat geen andere informatie bevat dan bedoeld onder a t/m c.

12.4 De persoonsgegevens worden slechts verstrekt aan:

 a. degenen, waaronder begrepen derden, die zijn belast met of leiding geven aan de in het tweede lid bedoelde activiteiten of die daarbij noodzakelijk zijn betrokken;

 b. anderen, in de gevallen bedoeld in artikel 8, onder a, c en d, en artikel 9, derde lid, van de

 Wbp.

12.5 De persoonsgegevens worden verwijderd op een daartoe strekkend verzoek van de betrokkene of bij diens overlijden.

**13. Klachten**

13.1. Indien de betrokkene van mening is dat de bepalingen van de Wbp zoals uitgewerkt in dit reglement niet door de instelling worden nageleefd dient hij zich te wenden tot de verantwoordelijke.

13.2. Indien de ingediende klacht voor de betrokkene niet leidt tot een voor hem acceptabel resultaat, kan de betrokkene zich wenden tot de klachtencommissie van [instelling] p/a ……., met het verzoek te bemiddelen of te adviseren in zijn geschil met de verantwoordelijke. Dit dient te geschieden binnen een termijn van twee weken na ontvangst van het antwoord van de verantwoordelijke.

**14. Inwerkingtreding en citeertitel**

Dit reglement kan aangehaald worden als privacyreglement medewerkers en treedt in werking op <datum invullen>.

Het reglement is vastgesteld door het bevoegd gezag en vervangt eventuele vorige versies.

**Bijlage 3:**

**Protocol social media voor deelnemers**

**Inleiding**

Sociale media spelen een belangrijke rol in het leven van deelnemers en medewerkers. Het gebruik van sociale media is onderdeel van het gedrag van deelnemers binnen de school. Sociale media kunnen helpen om het onderwijs te verbeteren en de lessen interessanter te maken, om contact te houden met vrienden en grenzen te verleggen. Aan het gebruik van sociale media kleven ook risico’s, zoals pesten en het ongewild delen van foto’s of andere gegevens. Met dit reglement kan het gesprek op school, in de klas en thuis gevoerd worden over wat er ‘gewoon’ is op sociale media (en wat niet). De afspraken zijn van toepassing op alle deelnemers van [instelling]. De afspraken zijn van toepassing op het gebruik van mobiele telefoons en sociale media op school en in de klas, maar ook bij social mediagebruik buiten de school.

**Scope**

Bij het gebruik van sociale media gaat het om programma’s waarmee online informatie kan worden opgezocht, gedeeld en gepresenteerd. Denk bijvoorbeeld aan Facebook, Twitter, Instagram, YouTube, Snapchat en alle (nieuwe) hiermee vergelijke programma’s en apps.

**Afspraken bij het gebruik van internet en sociale media**

Dit reglement is van toepassing op alle deelnemers van [instelling], onafhankelijk van de plaats waar zij hun sociale media gebruiken.

* *We behandelen elkaar netjes en met respect, en laten iedereen in zijn waarde. Daarom pesten, kwetsen, stalken, bedreigen en beschadigen we elkaar niet. We maken elkaar niet zwart.*
* Iedereen is verantwoordelijk voor wat hij/zij zelf plaatst op sociale media, en kan daarop aangesproken worden. Ook het doorsturen (forwarden) en herplaatsen (retweeten) zijn handelingen waar je op aangesproken kunt worden.
* Zorg dat je weet hoe de sociale media werken voordat je ze gebruikt, zorg dat de instellingen goed staan en je niet meer informatie deelt dan je wilt. Alles wat wordt gecommuniceerd via internet en sociale media, blijft nog lang vindbaar.
* Bij het gebruik van internet en sociale media houden we rekening met de goede naam van [instelling] en iedereen die daarbij betrokken is zoals docenten, onderwijsondersteunend personeel en externen ingehuurd door [instelling].
* We helpen elkaar om goed en verstandig met sociale media om te gaan, en we spreken elkaar daarop aan. Als dat niet lukt, dan vragen we daarvoor hulp aan onze leraar of mentor, afdelingscoördinator of directeur.
* Deelnemers en medewerkers van [instelling] worden geen ‘vriend’ of ‘contact’ van elkaar op sociale media, tenzij het gaat om een door de medewerkers gebruikt professioneel account (waar geen persoonlijke informatie over de medewerker is geplaatst).

***Opties:***

[De docent moet vooraf toestemming geven om een mobiele telefoon of sociale media in de les te gebruiken. Tijdens examens, toetsen, overhoringen en proefwerken gelden aangepaste regels.]

of:

[Het meenemen van mobiele telefoon en daarmee vergelijkbare communicatieapparatuur op school is [wel/niet] toegestaan. Een docent kan in verband met het leerproces deelnemers toestemming geven -om een mobiele telefoon mee te nemen en te gebruiken in de klas.]

of:

[Het gebruik van internet en sociale media is alleen toegestaan in de openbare ruimtes van [instelling] zoals de kantine, gangen en garderobe. Tijdens schoolactiviteiten zoals excursies is het gebruik van internet en sociale media alleen toegestaan tijdens de heen- en terugreis.]

* We respecteren elkaars privacy. Bij het gebruik van internet en sociale media worden er daarom geen informatie, foto’s of video’s verspreid over anderen, als zij daar geen toestemming voor hebben gegeven, of als zij daar negatieve gevolgen van kunnen ondervinden.

**Internet en sociale media worden alleen gebruikt voor acceptabele doeleinden. Het is daarom niet toegestaan om op school:**

* sites te bezoeken of informatie te downloaden en te verspreiden die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend zijn;
* te hacken en ongeoorloofd toegang te krijgen tot niet-openbare sites of programma’s;
* informatie, foto’s of video’s te delen waarvan duidelijk is dat die niet bedoeld is om verder te verspreiden, houd daarom je wachtwoorden geheim;
* verzonnen berichten te versturen of een fictieve naam te gebruiken als afzender;
* iemand lastig te vallen, te achtervolgen of te ‘flamen’.

Als iemand over de voorgaande punten informatie krijgt aangeboden, wordt dat gemeld aan de [leraar/mentor] of de [meldpunt].

Als er geconstateerd wordt dat de afspraken niet worden nageleefd, wordt dit eerst met de betrokkene besproken. Bij een ernstige overtreding kan de directie van [instelling] besluiten een maatregel op te leggen, die kan bestaan uit het uitsluiten van toegang tot het netwerk van de school, het in beslag nemen van de telefoon, het geven van een disciplinaire maatregel (straf) of in het uiterste geval het schorsen of verwijderen van de deelnemer van school.

Daarnaast kan de directie contact opnemen met de politie indien er (mogelijk) sprake is van een strafbaar feit. Zo nodig wordt aangifte gedaan.

[1-9-2016, versie 0.1]

*Dit model is bedoeld om het gesprek over het gedrag van deelnemers op school te stimuleren. Deze teksten dienen als inspiratie, maar kunnen ook integraal worden overgenomen. Het modelreglement is breed opgesteld. Deze versie kan ook van toepassing worden verklaard op onderwijzend en onderwijsondersteunend personeel. Dit kan door in artikel 1 toe te voegen dat het reglement van toepassing is op leraren/docenten en onderwijsondersteunend personeel van de school.*

Verwijzing naar documenten SCIPR











**Bijlage 4: Framework informatiebeveiliging en privacy in het mbo**



1. Onder ICT-middelen wordt onder meer verstaan: PC’s (computers), laptops, tablets, smartphones, usb-sticks, randapparatuur, smartboards, netwerk en netwerkcomponenten. [↑](#footnote-ref-1)