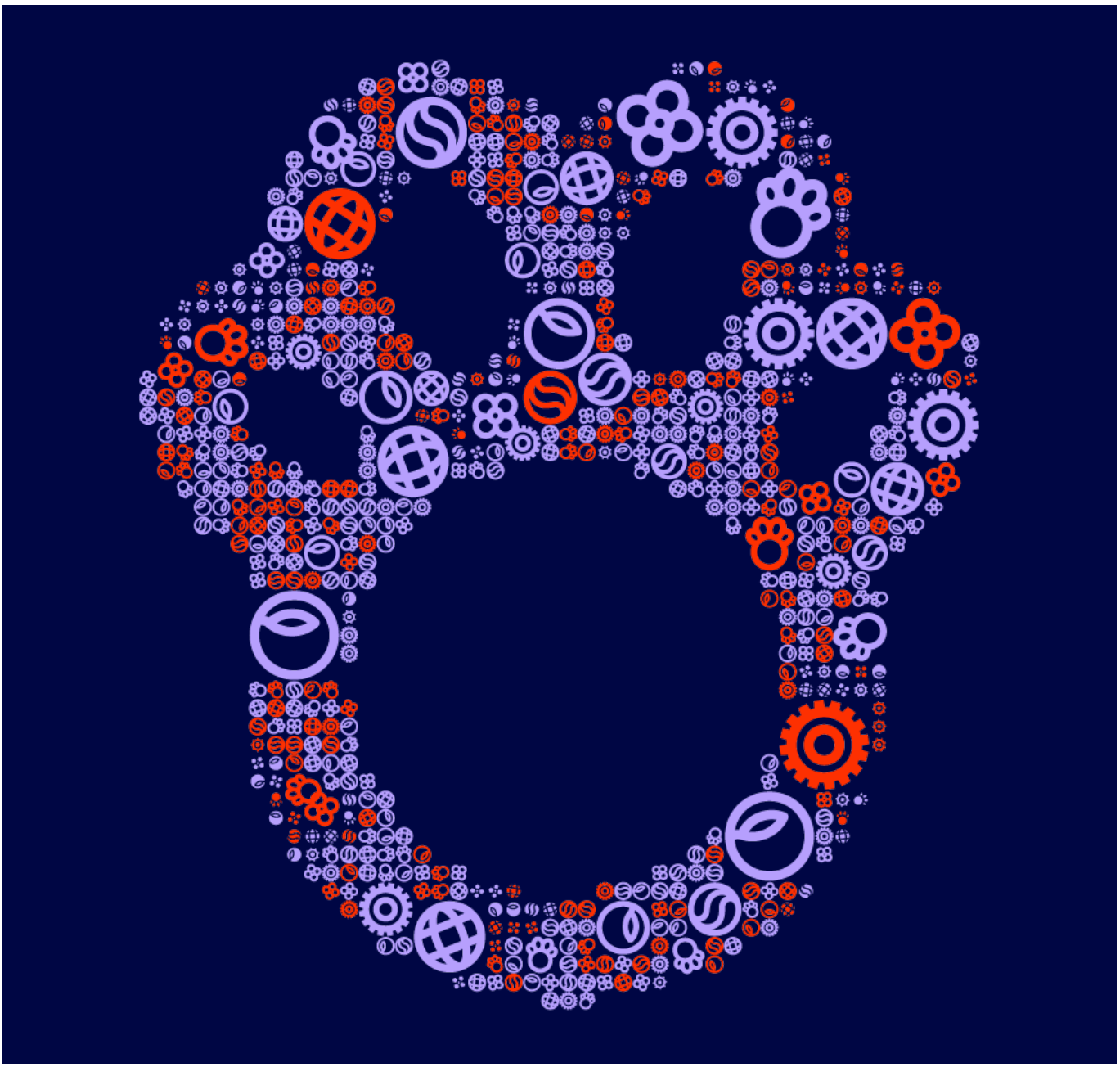

Reglement Verantwoord Netwerkgebruik

voor deelnemers

Dit beleid is op 25 april 2022 vastgesteld door het college van bestuur, en daarop volgend hebben de Centrale studentenraad en Centrale ouderraad instemming verleend.

Datum	25 april 2022
Versie	Vastgesteld

Yuverta

Colofon

Status
Vastgesteld

Locatie
De meest actuele vastgestelde versie staat op Yunet [klik hier].

Feedback
ibploket@yuverta.nl

Accordering
Welke organisatieonderdelen ontvangen het laatste concept ter kennisname en/of feedback, en welke organisatieonderdelen hebben instemmingsrecht.

Wie	*Laatste concept ter*	*Instemming**
College van Bestuur	kennisname / feedback	25-04-2022 [document]
Centrale studentenraad	kennisname / feedback	05-07-2022 [document]
Centrale ouderraad	kennisname / feedback	18-05-2022 [document]
Stafdirecteuren	kennisname / feedback	
Werkgroep Schoolveiligheid	kennisname / feedback	

* Waar een datum is ingevuld is dat de officiële datum van instemming.

Updatecyclus
Dit document wordt elke 2 jaar op actualiteit getoetst. De eerstvolgende herziening zal in 2023 plaatsvinden. Wanneer de situatie daar voldoende urgente aanleiding toe geeft wordt het document tussentijds bijgesteld.

Versie	*Status*	*Datum*	*Auteur*	*Omschrijving*
1.0	Definitief	10-07-2022	Alex Peeters, FG	Reglement gepubliceerd

Inhoudsopgave

1. Inleiding

Yuverta biedt aan leerlingen, studenten, en cursisten (hierna deelnemers) de mogelijkheid om voor hun studie gebruik te maken van onze ICT-faciliteiten. Zo hebben leerlingen en studenten de mogelijkheid om internet te gebruiken en worden voor persoonlijk gebruik een instellingsgebonden e-mailbox en digitale kantooromgeving beschikbaar gesteld.

Aan het gebruik van onze faciliteiten zijn regels verbonden. Deze regels zorgen ervoor dat onze faciliteiten beschikbaar zijn en voortdurend veilig gebruikt kunnen worden. Deze regels zijn in dit reglement opgenomen. Deze regels zijn van toepassing op iedereen die als leerling, student of cursist aan Yuverta is verbonden. Daarnaast zijn deze regels van toepassing op alle gasten die vanwege een verbintenis met een andere instelling via Eduroam en soortgelijke initiatieven van onze faciliteiten gebruik maken.

Yuverta streeft ernaar een goede balans aan te brengen tussen verantwoord en veilig ICT-gebruik en de privacy van deelnemers, medewerkers en gasten.

Om te controleren of onze faciliteiten niet worden gebruikt op een manier die in strijd is met de wet of andere geldende regels en om te zorgen dat onze faciliteiten altijd veilig zijn en niet overbelast worden, kan Yuverta het gebruik van haar faciliteiten bewaken op de manieren zoals beschreven in dit reglement.

2. Definities

In dit document worden de volgende definities gehanteerd:

Faciliteiten: alle ICT-faciliteiten van Yuverta waaronder (draadloze) (internet) verbindingen en andere infrastructuur, (cloud-) applicaties en -toepassingen en de (persoons-) gegevens die daarin zijn opgeslagen, online presence, apparatuur met netwerk, opslag- en/of rekencapaciteit, printers etc.

Deelnemer: eenieder die als leerling, student of cursist aan Yuverta is verbonden.

Medewerker: eenieder die als vaste, tijdelijke, ingehuurde, gedetacheerde werknemer, stagiair, vrijwilliger of als medewerker van een leverancier aan Yuverta is verbonden.

Gast: eenieder die via een extern of tijdelijk account gebruik maakt van onze faciliteiten.

Gebruiker: deelnemer of gast welke van onze faciliteiten gebruik maakt.

Reglement: dit document. Naast dit document heeft Yuverta ook een soortgelijk reglement voor medewerkers.

Authenticatiemiddelen: gebruikersnaam, wachtwoord en in sommige gevallen een tweede authenticatie factor.

Instelling: onderwijsinstelling Yuverta.

Locatie: school- en stafdienst locaties van Yuverta en locaties waar Yuverta overig onderwijs, stages, excursies en schoolreizen verzorgt.

Waar deze bijzondere woorden hierna in de tekst gebruikt worden zijn deze groen gemarkeerd.

3. Gebruik van de faciliteiten

Yuverta stelt faciliteiten beschikbaar ten behoeve van de studie, onder meer voor het kunnen maken van opdrachten, verslagen en scripties, het bijhouden van de studievoortgang, het raadplegen van bronnen en het communiceren met medewerkers en andere deelnemers.

Het gebruik van eigen apparatuur en toepassingen op de faciliteiten van Yuverta is toegestaan, zolang dit gebruik voldoet aan de regels van dit reglement. Het veranderen van instellingen in faciliteiten welke door Yuverta beschikbaar zijn gesteld is niet toegestaan. Het aansluiten van apparatuur waarmee de faciliteiten met derden kunnen worden gedeeld is te allen tijde verboden.

Bepaalde faciliteiten zijn alleen toegankelijk met behulp van een gebruikersnaam en een wachtwoord en in sommige gevallen een aanvullend authenticatiemiddel (zoals authenticator app, smartcard of token). Deze authenticatiemiddelen zijn strikt persoonsgebonden en mogen niet met anderen worden gedeeld. Bij een vermoeden van misbruik van inloggegevens, houdt de instelling zich het recht voor, al dan niet geautomatiseerd, maatregelen tegen misbruik te nemen. Disciplinaire maatregelen kunnen genomen worden wanneer blijkt dat er sprake is van opzet, bijvoorbeeld wanneer de eigenaar van het account het wachtwoord opzettelijk heeft gedeeld met anderen.

3.1 Beveiliging door de instelling en de deelnemer

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

Natuurlijk is een perfecte beveiliging onmogelijk. Daarom verwacht Yuverta ook van gebruikers van onze faciliteiten een proactieve houding en serieuze stappen om de eigen computer en andere apparatuur (zoals eigen smartphones of eigen tablets) adequaat te beveiligen. Zo is eenieder te allen tijde zelf verantwoordelijk voor het gebruik van de eigen apparatuur en de op deze apparatuur opgeslagen gegevens.

Eenieder die met eigen apparatuur gebruik maakt van onze faciliteiten, draagt persoonlijk zorg voor adequate beveiliging van de eigen apparatuur. Dit gebeurt door:

- deze apparatuur te voorzien van een up-to-date virusscanner;
- onrechtmatige toegang tot gegevens en systemen van Yuverta te voorkomen door moeilijk te raden wachtwoorden en/of pincodes te gebruiken;
- deze hard- en software regelmatig met updates bij te houden;
- Gebruik Apple Filevault of Microsoft Bitlocker etc. om opgeslagen gegevens op de interne opslag van het apparaat te beveiligen door middel van versleuteling.

3.2 Privégebruik en overlast

Hoewel de faciliteiten bedoeld zijn voor gebruik ten behoeve van de studie, is privégebruik toegestaan. Gebruik van onze faciliteiten moet te allen tijde:

- niet illegaal, storend of overlast veroorzakend zijn;
- geen studiehinder bij jezelf of anderen veroorzaken;
- geen aantasting vormen voor de integriteit en de veiligheid andere personen of van de faciliteiten.

Onder illegaal, storend, onrechtmatig 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 blijk geven van of (kunnen) aanzetten tot discriminatie, haat en/of geweld;
- het versturen van berichten aan grote aantallen ontvangers tegelijk, het versturen van kettingbrieven;
- het verspreiden of installeren van kwaadaardige hard- of software zoals keyloggers, virussen, wormen, Trojaanse paarden en spyware;
- filesharing- of streamingdiensten te gebruiken wanneer dit overmatig veel dataverkeer genereert, zodanig dat het de beschikbaarheid van de faciliteiten kan aantasten;
- opslaan van grote hoeveelheden privégegevens of -bestanden. Yuverta is tevens niet verplicht van dergelijke bestanden of informatie reservekopieën te maken of kopieën beschikbaar te stellen bij vervanging of reparatie van de betreffende systemen.

3.3 Intellectueel eigendomsrecht

Eenieder die gebruik maakt van onze faciliteiten maakt daarbij geen inbreuk op de intellectuele eigendomsrechten van Yuverta en van derden en respecteert de licentie afspraken zoals die binnen Yuverta van toepassing zijn.

De zeggenschap over de informatie van Yuverta berust bij het college van bestuur. De deelnemer heeft geen zelfstandige zeggenschap over de informatie behalve als hem/haar dat expliciet is toegekend.

Yuverta geeft haar deelnemers beschikbaarheid over een digitale bibliotheek. De inhoud van deze bibliotheek wordt uitsluitend ten behoeve van de studie ter beschikking gesteld. Het is niet toegestaan inhoud van de digitale bibliotheek voor andere doeleinden te kopiëren of verspreiden.

3.4 Vertrouwelijke informatie

Indien de deelnemer in het kader van zijn studie of het uitvoeren van taken voor de instelling toegang krijgt tot vertrouwelijke of privacygevoelige informatie, dient de deelnemer die informatie strikt vertrouwelijk te behandelen.

De deelnemer besteedt bijzondere aandacht aan het treffen van beveiligingsmaatregelen, indien in het kader van het uitvoeren van studie of andere taken de verwerking van persoonsgegevens of vertrouwelijke informatie buiten de instelling noodzakelijk is. Het is niet toegestaan persoonsgegevens of vertrouwelijke informatie op te slaan:

- in niet instellingsgebonden cloud-toepassingen;
- in cloud-toepassingen waarvoor geen verwerkersovereenkomst is afgesloten;
- op externe opslagmedia (externe harddisks, usb-sticks);
- op onversleutelde eigen apparatuur.

Indien de instelling met betrekking tot het waarborgen van de vertrouwelijkheid en de intellectuele eigendomsrechten nadere voorschriften heeft opgesteld, dienen deze door eenieder die van onze faciliteiten gebruik maakt stipt te worden opgevolgd.

3.5 Afstandsonderwijs

Yuverta heeft de wettelijk verplichting om aanwezigheid (participatie) bij de les te controleren en te registreren. In de digitale omgeving is hiervoor de keuze gemaakt dit middels een combinatie van beeld en geluid te doen. Omdat die controle met stem alleen onvoldoende zeker is, moet middels beeld gecontroleerd of de juiste persoon aan de les meedoet. Dit is een zwaarwegend belang.
Om de privacy impact te minimaliseren is het toegestaan en zelfs aangeraden om een achtergrond in te stellen.

Studenten houden zich aan onderstaande aanwijzingen:

- Luister altijd naar de instructies van de docent.
- Neem geen lessen op of maak ook niet met jouw telefoon of op andere manieren opnames van jouw docent of medestudent. Net zoals dit ook in een normale les niet mag, mag dit ook niet tijdens een digitale les.
- Overtredingen van de regels kunnen, net zoals tijdens reguliere lessen, worden bestraft met de gangbare disciplinaire maatregelen.
- Om je aanwezigheid te registreren zet je je camera aan als de docent hierom vraagt.
- Om de privacy van jezelf en anderen te beschermen raden we je aan je achtergrond te vervagen of anders in te stellen.

3.6 Social Media

Social media is een verzamelnaam voor alle internettoepassingen die het mogelijk maken om informatie met elkaar te delen op een eenvoudige en vaak leuke manier. Het gaat hierbij niet alleen om informatie in de vorm van tekst (nieuws, artikelen). Ook geluid (podcasts, muziek) en beeld (fotografie, video) worden gedeeld via social media (Instagram, YouTube, Facebook, Twitter, Snapchat, TikTok, enz.). De essentie van social media is dat iemand er informatie deelt over zichzelf, over anderen of over een bepaald onderwerp. Voor gebruik van social media geldt als uitgangspunt dat het digitale gedrag op social media niet afwijkt van het real life gedrag binnen de school.

Bij Yuverta gelden naast de regels in artikel 3.2, de volgende afspraken voor het gebruik van social media:

- ✓ Deel op verantwoorde wijze kennis via social media rekening houdend met de goede naam van Yuverta en iedereen die hierbij betrokken is.
- ✓ Publiceer geen vertrouwelijke informatie op social media.
- ✓ Publiceer geen beeldmateriaal of andere persoonsgegevens zonder de uitdrukkelijke voorafgaande aantoonbare toestemming van betrokkenen. Van ouders als de deelnemers jonger is dan 16 jaar, of van de deelnemer zelf, als deze ouder is dan 16 jaar.
- ✓ Wees je ervan bewust dat publicaties op social media altijd vindbaar (openbaar) en moeilijk vernietigbaar zijn.
- ✓ Vermijd online (negatieve) discussies en meningsverschillen. Bespreek deze in-real-life met de betrokkenen.
- ✓ Deelnemers zijn persoonlijk verantwoordelijk voor wat zij publiceren. Neem contact op met je mentor, coach of docent als er twijfel bestaat over een publicatie of over de raakvlakken met Yuverta.

- ✓ Wanneer social media in het lesprogramma wordt ingezet gebeurt dit uitsluitend op basis van vrijwillige deelname. Wanneer leerlingen jonger zijn dan 16 jaar, uitsluitend na toestemming van ouders.

Als Yuverta signalen ontvangt dat bovenstaande regels niet zijn nageleefd dan kan hier nader onderzoek naar worden ingesteld. Hierbij wordt uitsluitend gebruik gemaakt van informatie in openbare bronnen; hieronder vallen ook bronnen die door derden aan Yuverta worden geopenbaard. Dit onderzoek zal plaatsvinden onder de voorwaarden zoals opgenomen in artikel 5.

4. Melden van beveiligingsincidenten en datalekken

Van alle deelnemers wordt verwacht dat zij beveiligingsincidenten en mogelijke datalekken melden volgens de geldende procedure van Yuverta.

5. Controle door de instelling

Yuverta controleert de naleving van dit reglement. Yuverta handelt bij de controle op het gebruik van de faciliteiten binnen de geldende wet- en regelgeving.

Yuverta streeft in het kader van de controle en handhaving van dit reglement naar maatregelen, die inzage in privacygevoelige informatie of persoonsgegevens zo veel mogelijk beperken. Yuverta zal daarbij uitgaan van de juiste balans tussen verantwoord gebruik van de faciliteiten en de bescherming van de privacy van eenieder die van onze faciliteiten gebruik maakt. Zij zal, waar mogelijk, slechts geautomatiseerd controleren of filteren, zonder daarbij zichzelf of andere personen inzage te geven in gedrag van individuele personen.

5.1 Voorwaarden voor controle

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 binnen de instelling, de bewaking van de integriteit en de veiligheid van de faciliteiten. Verboden gebruik van de faciliteiten wordt zo veel mogelijk langs technische weg onmogelijk gemaakt.

Ten behoeve van deze controle worden geautomatiseerd gegevens verzameld (gelogd). Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens, die niet herleidbaar zijn tot identificeerbare personen. De gegevens, die uit een dergelijke controle voortkomen, 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 faciliteiten te kunnen gebruiken.

In het bijzonder kan bij overlast, veroorzaakt door apparatuur van eenieder die onze faciliteiten gebruikt, worden overgegaan tot uitschakeling van de netwerktoegangsmogelijkheden. Indien mogelijk wordt de gebruiker 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 men zo snel mogelijk melding van de maatregel.

Bij vermoedens van overtreding van de regels kan gedurende een vastgestelde (korte) periode, gerichte 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 procedure bij gericht onderzoek, wordt hieronder bij 5.2 beschreven.

Yuverta houdt zich bij het controleren op het niveau van verkeersgegevens of de inhoud onverkort aan de Algemene verordening gegevensbescherming (AVG) 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.

Persoonsgegevens, die zijn vastgelegd in het kader van toezicht en controle, worden bewaard voor een zo kort mogelijke periode. Enkel indien er een redelijk vermoeden bestaat van onrechtmatig gebruik kan deze periode worden verlengd.

Zodra een onderzoek is afgerond en niet leidt tot maatregelen tegenover een betrokkene, worden de gegevens verwijderd.

5.2 Uitvoering van de controle

Om controle uit te kunnen voeren op de naleving van dit reglement, kan de instelling enkele specifieke maatregelen treffen. Zo vindt de controle op het uitlekken van vertrouwelijke informatie, waartoe de deelnemer in het kader van zijn studie of het uitvoeren van taken voor Yuverta toegang heeft, plaats op basis van steekproefsgewijze contentfiltering. Verdachte berichten worden apart gezet voor nader onderzoek.

Daarnaast wordt de controle in het kader van kosten- en capaciteitsbeheersing beperkt tot het op basis van verkeersgegevens nagaan van de bronnen van kosten of capaciteitsvraag (zoals de adressen van internetradio en videosites of omvang van mappen in het opslagsysteem). Waar het gebruik van deze faciliteiten tot grote kosten of overlast leiden, worden beperkende maatregelen getroffen, zonder daarbij de vertrouwelijkheid van de inhoud van de communicatie te schenden;

De afdeling ICT en de systeembeheerder(s) zijn aan geheimhouding gebonden als men in het kader van de controle op dit reglement om technische redenen kennis moet nemen van persoonsgebonden informatie, behalve als enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.

Yuverta treft in het kader van de controle op dit reglement de nodige maatregelen, opdat persoonsgegevens, gelet op de doeleinden waarvoor zij verwerkt worden, juist en nauwkeurig zijn.

Yuverta treft in het kader van de controle op dit regelement passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies en/of tegen enige vorm van onrechtmatige verwerking.

5.3 Procedure bij gericht onderzoek

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

Gericht onderzoek vindt uitsluitend plaats na schriftelijke opdracht van de directeur van de betreffende regio of stafdienst. Het college van bestuur en de Functionaris voor Gegevensbescherming ontvangen 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.

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

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 het college van bestuur, welke toestemming de redenen zal noemen waarom deze wordt verleend.

Enkele specifieke persoonsgebonden maatregelen ter controle die de instelling kan voeren, zijn:

- De controle op overtreding van het verbod uit artikel 3.2 vindt door twee personen plaats door, op basis van een klacht, e-mailberichten te openen en de inhoud te raadplegen. Deze personen zijn gebonden aan geheimhouding over de inhoud.
- De gebruiker wordt zo spoedig mogelijk schriftelijk geïnformeerd door de directeur van de betreffende regio of stafdienst over de aanleiding, de uitvoering en het resultaat van het onderzoek. De gebruiker wordt in de gelegenheid gesteld uitleg te geven over de aangetroffen gegevens. Uitstel van het informeren mag alleen als informeren de kwaliteit van het onderzoek daadwerkelijk zou schaden.

Systeembeheerders verschaffen zich slechts toegang tot accounts of computers van gebruikers als de gebruiker 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, en op basis van toestemming van de directeur van de betreffende regio, zoals nader bepaald in dit artikel. De gebruiker zal in dat geval achteraf worden geïnformeerd.

6. Consequenties van overtreding van dit reglement

Bij handelen in strijd met dit reglement of de algemeen geldende wetgeving bij het gebruik van de faciliteiten, kan het college van bestuur, afhankelijk van de aard en de ernst van de overtreding, disciplinaire maatregelen treffen welke zijn benoemd in het leerlingen- en studentenstatuut.

Zoals een mondelinge of schriftelijke waarschuwing/berisping, een afsluiting of beperking van toegang tot de faciliteiten, schorsing, en in extreme gevallen een beëindiging van de inschrijving als deelnemer.

Zulke disciplinaire maatregelen kunnen niet worden getroffen enkel op basis van een langs geautomatiseerde weg uitgevoerde besluitvorming, zoals een constatering van een automatisch filter. Voorts worden geen disciplinaire maatregelen getroffen zonder dat de gebruiker gelegenheid heeft gekregen zijn zienswijze naar voren te brengen.

Maatregelen zoals een waarschuwing en een gerichte blokkade waarbij sprake is van real-time blokkeren ter voorkoming van verstoring van orde of veiligheid, zoals bij blokkeren van malware, kunnen op basis van geautomatiseerde besluitvorming worden genomen. Deze blokkade zal maximaal een week worden gehandhaafd of korter als de oorzaak naar tevredenheid van het systeembeheer van Yuverta is weggenomen. Indien na een week geen verbetering is geconstateerd door het systeembeheer, kan het systeembeheer besluiten tot een langere blokkade. Bij herhaling van de oorzaak kunnen disciplinaire maatregelen worden genomen.

Yuverta is te allen tijde gerechtigd om aangifte te doen van geconstateerde strafbare feiten.

7. Rechten met betrekking tot persoonsgegevens

De rechten van betrokkenen zoals die in de AVG beschreven zijn gelden uiteraard ook hier. In dit hoofdstuk beschrijven we deze rechten, en op welke wijze je deze kunt uitoefenen.

De deelnemer kan zich tot het college van bestuur wenden met het verzoek om een volledig overzicht van zijn persoonsgegevens, zoals door de instelling verwerkt in het kader van dit reglement.

De deelnemer kan het college van bestuur verzoeken zijn persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen, indien deze feitelijk onjuist zijn, voor het doel onvolledig of niet ter zake dienend zijn, dan wel het verwerken ervan in strijd met een wettelijk voorschrift is.

De deelnemer kan verder bezwaar maken tegen de verwerking van zijn persoonsgegevens, indien er sprake is van bijzondere persoonlijke omstandigheden. In dat geval zal de verwerking gestopt, dan wel beperkt worden, tenzij er sprake is van dwingende gerechtvaardigde belangen, die zwaarder wegen dan de rechten en vrijheden van de deelnemer.

De deelnemer heeft in sommige gevallen het recht om het verwerken van zijn persoonsgegevens (al dan niet tijdelijk) te beperken. De deelnemer kan de verwerking van zijn persoonsgegevens beperken, indien de gegevens mogelijk onjuist zijn, de verwerking onrechtmatig is, de gegevens niet meer nodig zijn, dan wel de deelnemer bezwaar tegen de verwerking heeft ingediend.

De deelnemer kan het college van bestuur verzoeken zijn persoonsgegevens te verwijderen indien deze niet meer nodig zijn, hij eerder toestemming heeft gegeven voor het gebruik van zijn gegevens maar deze toestemming nu intrekt, hij bezwaar gemaakt heeft tegen de verwerking, de verwerking onrechtmatig is, dan wel de wettelijk bepaalde bewaartermijn verlopen is.

Indien dit technisch mogelijk is, heeft de deelnemer tevens het recht om de persoonsgegevens, die de instelling in het kader van dit reglement van hem verwerkt, te laten overdragen naar een derde partij.

De deelnemer heeft daarnaast het recht op een menselijke blik bij besluiten op basis van automatisch verwerkte gegevens.

Op bovengenoemde verzoeken wordt binnen vier weken gereageerd. Deze termijn kan echter met twee maanden worden verlengd om redenen die verband houden me de specifieke privacy rechten of de complexiteit van het verzoek. Van een dergelijke verlenging van de termijn zal het college van bestuur de deelnemer binnen vier weken op de hoogte stellen. Een weigering is met redenen omkleed. Een toegewezen verzoek zal zo spoedig mogelijk worden uitgevoerd.

8. Slotbepalingen

Dit reglement wordt jaarlijks geëvalueerd door inhoudelijke kennisexperts. Wanneer nodig wordt een herziene versie vastgesteld door het college van bestuur.

De organisatie kan dit reglement, met instemming van het Centrale studentenraad en Centrale ouderraad, wijzigen als de omstandigheden daar aanleiding toe geven. Voorgenomen wijzigingen worden voorafgaand aan de invoering aan de leerlingen, studenten en cursisten bekend gemaakt. Het college van bestuur zal feedback van leerlingen, studenten en cursisten in overweging nemen alvorens de wijzigingen in te voeren.

In gevallen waarin dit reglement niet voorziet, beslist het college van bestuur.