Gedragscode ICT

Bestuur

scholengemeenschap voor
vmbo
havo
atheneum
gymnasium

school voor
praktijkonderwijs

Afspraken i.v.m. veranderende wetgeving (de Algemene Verordening Gegevensbescherming), met ingang van 25 mei 2018.
Deze regeling is door het bevoegd gezag vastgesteld op 27 juni 2018, na instemming van de GMR op 25 juni 2018.

Bezoekadres:
Stationslaan 17
9503 CA Stadskanaal

Postadres:
Postbus 137
9500 AC Stadskanaal

0599 - 631122

Inhoud

1. Inleiding 3

2. Uitgangspunten 4

2.1. Uitgangspunten gedragscode 4
2.2. Eigen verantwoordelijkheid en privégebruik 4
2.3. Verschillende soorten gegevens 5

3. Intellectueel eigendom en vertrouwelijke informatie 6

4. Algemene normen gedragscode 6

5. Gebruik van computer- en netwerkfaciliteiten 7

5.1. Werkplek 7
5.2. Gebruik eigen devices (BYOD) 8
5.3. Software en digitaal lesmateriaal 9

6. Gebruik van e-mail en andere ict-communicatiemiddelen 9

7. Gebruik van internet 10

7.1. Veilig online 11
7.2. Sociale media 11
7.3. Gebruik beeld- en geluidsmateriaal 12
7.4. Wachtwoorden en pincodes 12
7.5. Meldplicht Datalekken 13

8. Monitoring en controle 13

8.1. Voorwaarden voor controle 13
8.2. Uitvoering van de controle 14
8.3. Disciplinaire maatregelen 14
8.4. Bezwaar en beroep 15

9. Slotbepaling 15

1. Inleiding

Het gebruik van internet en ICT-middelen is voor (veel van) de leerlingen en werknemers noodzakelijk om hun werk goed te kunnen doen of aan lesactiviteiten deel te nemen. Aan het gebruik hiervan zijn echter risico's verbonden die vragen om het maken van afspraken over gedragsregels. Tegen de achtergrond van deze risico's mag van de leerlingen en werknemers verantwoord gebruik van internet en ICT-middelen worden verwacht. De stichting is als werkgever en onderwijsinstelling bevoegd regels te stellen omtrent de uitvoering van werk en lesactiviteiten en de goede orde op de werkvloer en in de klas.

Met deze gedragscode willen we als stichting Ubbo Emmius regels stellen omtrent het gewenst gebruik van de bedrijfsmiddelen. Het streven daarbij is een goede balans aan te brengen tussen verantwoord en veilig ICT- en internetgebruik en de privacy van de leerling en werknemer.

Het gebruik van sociale media zoals Facebook, LinkedIn en Twitter is niet meer weg te denken uit de huidige maatschappij, maar kan ook zijn weerslag hebben op het gebruik van ICT-middelen. Daarom gelden ook hiervoor bepaalde regels. De richtlijnen voor sociale media zijn beschreven in een apart document, het 'Protocol Sociale Media'.

De (ict)faciliteiten en de verschillende gegevens worden in dit document ook bedrijfsmiddelen genoemd. Onder bedrijfsmiddelen worden in ieder geval verstaan:

- Hardware: pc, laptop, tablet, telefoon, hardware token (tag).
- Software (of -systemen): alle applicaties voor het uitvoeren van de werkzaamheden, zoals de school e-mailomgeving, Microsoft Office, administratiesystemen en (online)digitaal lesmateriaal maar ook apps op (mobiele) devices.
- Informatie en (persoons)gegevens: rapportages, leerlingdossiers, gegevens in e-mails. Hierbij vraagt de verwerking van persoonsgegevens vanuit de privacywetgeving extra maatregelen.
- Internetgebruik: het bezoeken van het World Wide Web, het gebruik van e-mail en diensten als FTP maar ook sociale media zoals Facebook, LinkedIn, Instagram en Twitter.

Deze gedragscode moet gezien worden als een nadere uitwerking van het Informatiebeveiligings- en privacybeleid van de stichting Ubbo Emmius.

2. Uitgangspunten

2.1. Uitgangspunten gedragscode

Deze gedragscode stelt regels ten aanzien van het gebruik van de bedrijfsmiddelen ICT en internet door leerlingen, werknemers en bezoekers. Doel van deze regels is de goede orde te bepalen ten aanzien van:

- systeem- en netwerkbeveiliging, inclusief beveiliging tegen schade en misbruik;
- tegengaan van seksuele intimidatie, discriminatie en andere strafbare feiten;
- bescherming van privacygevoelige informatie waaronder persoonsgegevens van het schoolbestuur, haar medewerkers, leerlingen en hun ouders en daarmee het beschermen van de privacy en veiligheid van alle betrokkenen;
- bescherming van vertrouwelijke informatie van het schoolbestuur, haar medewerkers, leerlingen en hun ouders;
- het voorkomen en tegengaan van misbruik van de bedrijfsmiddelen;
- bescherming van de intellectuele eigendomsrechten van de stichting Ubbo Emmius en derden waaronder het respecteren van de licentie-afspraken die van toepassing zijn;
- voorkomen van negatieve publiciteit en
- kosten- en capaciteitsbeheersing.

Deze gedragscode geldt voor eenieder die gebruik maakt van netwerkvoorzieningen, dus voor leerlingen, medewerkers, maar ook voor tijdelijke werknemers (bijvoorbeeld uitzendkrachten en gedetacheerde werknemers), zelfstandigen en gasten.

De controle op het gebruik van bedrijfsmiddelen is een verwerking van persoonsgegevens in de zin van de privacywetgeving. De stichting Ubbo Emmius zal dan ook de controle en handhaving van deze regels conform de privacywetgeving en het algemene arbeidsrechtelijk kader uitvoeren. Hierbij is het uitgangspunt een goede balans tussen verantwoord gebruik van bedrijfsmiddelen en de bescherming van de privacy van medewerkers op de werkplek. Gegevens worden alleen verzameld en gebruikt voor deze doelen. In het bijzonder zal het bestuur de bij controle vastgelegde gegevens beveiligen tegen ongeautoriseerde toegang. Het bestuur zal mensen met toegang daartoe contractueel verplichten tot afdoende geheimhouding

We streven in het kader van handhaving van deze gedragscode naar maatregelen die inzage in privacygevoelige informatie of persoonsgegevens van individuele leerlingen of werknemers zo veel mogelijk beperken. We zullen bijvoorbeeld waar mogelijk slechts geautomatiseerd controleren of filteren zonder daarbij onszelf of andere personen inzage te geven in gedrag van individuele personen.

2.2. Eigen verantwoordelijkheid en privégebruik

Het gebruik van door de stichting Ubbo Emmius verstrekte bedrijfsmiddelen is persoonlijk en blijft de verantwoordelijkheid van de medewerker. Alle devices die voor schoolwerk worden gebruikt (inclusief

eigen devices ‘Own Device’) worden niet uitgeleend of aan anderen ter beschikking gesteld zonder aanvullende (beveiligings)maatregelen. Het niet voldoen aan de regels voor informatiebeveiliging en privacy kan leiden tot disciplinaire maatregelen.

2.3. Verschillende soorten gegevens

De stichting Ubbo Emmius is verantwoordelijk voor het regelen van informatiebeveiliging en privacy. Het belangrijkste doel van informatiebeveiliging en privacy is het beschermen van gegevens. De stichting onderscheidt drie typen gegevens:

- *Openbare gegevens*; dit zijn gegevens die juist voor publicatie bedoeld zijn.
- *Interne gegevens*; dit zijn gegevens die alleen voor gebruik en verwerking binnen de stichting Ubbo Emmius bedoeld zijn. Denk na voordat je deze gegevens deelt met externen.
- *Vertrouwelijke gegevens*; dit zijn gegevens die alleen voor specifieke, hiervoor geautoriseerde medewerkers binnen de stichting Ubbo Emmius toegankelijk zijn. Denk hierbij aan (bijzondere) persoonsgegevens, personeelsgegevens of aanbestedingsgegevens.

Persoonsgegevens verdienen bijzondere aandacht. Dit zijn gegevens die een persoon betreffen én waardoor een persoon geïdentificeerd of identificeerbaar is. Denk hierbij aan naamgegevens, emailadressen maar ook telefoonnummers van zowel collega’s als leerlingen en ouders van leerlingen. De privacywetgeving verplicht elk individu om zorgvuldig met persoonsgegevens om te gaan. Een onderdeel van de wettelijke verplichting is dat de stichting Ubbo Emmius schriftelijk afspraken maakt met leveranciers van (online)applicaties, waarbij persoonsgegevens worden verwerkt (denk hierbij aan inloggegevens, wachtwoorden en het opslaan van gemaakt werk).

De stichting Ubbo Emmius heeft een Functionaris voor gegevensbescherming aangesteld. Deze communiceert intern de gedragsregels die horen bij het verwerken van persoonsgegevens. Persoonsgegevens moeten altijd met uiterste zorgvuldigheid verwerkt en gedeeld worden.

Als persoonsgegevens toegankelijk en of inzichtelijk zijn voor personen die geen toegang behoren te hebben tot deze gegevens, is er sprake van een beveiligingsincident, waaruit mogelijk een datalek kan voortkomen. Een dergelijk incident kan schadelijke gevolgen hebben voor de betrokkene(n) en de stichting Ubbo Emmius. Om op een veilige, verantwoorde en werkbare manier met deze gegevens om te gaan maakt de stichting Ubbo Emmius afspraken over:

- de verwerking en verspreiding van vertrouwelijke- en persoonsgegevens. Er worden niet meer gegevens verwerkt dan noodzakelijk om het doel te bereiken;
- de uitwisseling van gegevens, waarbij aan de ontvanger wordt aangegeven wat de ontvanger wel of niet mag doen met de gegevens;
- opslag en verspreiding van gegevens, waarbij alléén gebruik gemaakt wordt van door de stichting Ubbo Emmius goedgekeurde bedrijfsmiddelen.

Van medewerkers van de stichting Ubbo Emmius en/of externe medewerkers, die uit hoofde van hun functie toegang hebben tot de digitale informatiesystemen en hiermee tot bv. personeelsdossiers, vertrouwelijke enquêtegegevens, zorgdossiers etc. wordt verwacht dat zij zorgvuldig omgaan met de

functioneel aan hen beschikbaar gestelde informatie en dat zij de privacywetgeving hanteren en op geen enkele wijze informatie, waarvan redelijkerwijze kan worden aangenomen dat deze vertrouwelijk of privacygevoelig is, zonder toestemming van betrokkene of leidinggevende te gebruiken en/of naar buiten te brengen.

3. Intellectueel eigendom en vertrouwelijke informatie

Werknemers dienen vertrouwelijke informatie, waar zij in het kader van het werk toegang toe hebben, strikt vertrouwelijk te behandelen en voldoende maatregelen te treffen om de vertrouwelijkheid te waarborgen.

Leerlingen en werknemers maken geen inbreuk op de intellectuele eigendomsrechten van de stichting Ubbo Emmius en derden en respecteren de licentie-afspraken zoals die van toepassing zijn.

Werknemers besteden bijzondere aandacht aan het treffen van maatregelen zoals in deze gedragscode genoemd, indien in het kader van het uitvoeren van de werkzaamheden de verwerking van vertrouwelijke informatie buiten Ubbo Emmius noodzakelijk is.

Deze bepalingen gelden in het bijzonder voor systeembeheerders, voor wie schending van deze bepalingen als een zeer ernstig plichtsverzuim wordt aangemerkt, gezien hun bijzondere positie.

4. Algemene normen gedragscode

In deze gedragscode voor verantwoord gebruik van bedrijfsmiddelen geeft de stichting Ubbo Emmius aan wat de afspraken zijn met betrekking tot verschillende onderwerpen rondom het gebruik van bedrijfsmiddelen en wat dit voor de medewerkers in de dagelijkse praktijk betekent.

Iedere medewerker voldoet aan de volgende algemene normen voor ‘zorgvuldigheid’ (niet uitputtend):

- Ga zorgvuldig om met persoonsgegevens, waarbij de basisregels voor het omgaan met persoonsgegevens als bekend worden geacht.
- Voorkom het lekken van interne en vertrouwelijke informatie.
- Zorg voor een goede fysieke en technische bescherming van bedrijfsmiddelen (beveiligingsmaatregelen).
- Voorkom dat beveiligingsmaatregelen moedwillig worden omzeild (bijvoorbeeld door jailbreaks).

- Meld diefstal of verlies van bedrijfsmiddelen onmiddellijk na constatering door het sturen van een e-mail of een telefonische melding bij je locatiedirecteur. (Zie verder de procedure Datalekken en de meldplicht van de stichting Ubbo Emmius).

5. Gebruik van computer- en netwerkfaciliteiten

Computer- en netwerkfaciliteiten (ict-bedrijfsmiddelen) worden aan leerlingen en medewerkers beschikbaar gesteld voor zover deze nodig zijn voor het uitvoeren van de dagelijkse werkzaamheden. Gebruik is derhalve verbonden aan taken die voortvloeien uit deze werkzaamheden. Bij het gebruik van de ict-bedrijfsmiddelen gelden de volgende afspraken:

- Zorg dat privacygevoelige gegevens niet toegankelijk zijn voor onbevoegden.
- Weet welke gegevens er mogen worden gebruikt (mag iedereen het zien?) en welke ict-voorzieningen kunnen worden ingezet (is het veilig genoeg?) bij het verrichten van de verschillende schoolwerkzaamheden.
- Sla (persoons)gegevens alleen op de daarvoor aangewezen systemen op. (Opslaan van gegevens in public Cloud omgevingen, zoals een persoonlijke dropbox, is niet toegestaan).
- Versleutel alle gegevens met betrekking tot de stichting Ubbo Emmius, indien deze gegevens, om welke reden dan ook, elders opgeslagen worden (denk hierbij ook aan een usb-stick).
- Leerlingen en werknemers dienen te allen tijde zorgvuldig om te gaan met aan hen persoonlijk toegekende inloggegevens en eventuele aanvullende authenticatiemiddelen. Persoonsgebonden wachtwoorden en aanvullende authenticatiemiddelen mogen niet worden gedeeld. Bij een vermoeden van misbruik van een wachtwoord kan het systeembeheer per direct het betrokken account ontoegankelijk maken.
- Sluit na gebruik de computer af of log uit.
- Het installeren van software op de computer- en netwerkfaciliteiten van de organisatie is niet toegestaan zonder aparte schriftelijke toestemming van het systeembeheer. Ook het aansluiten van servers en actieve netwerkcomponenten (zoals access points en routers) is niet toegestaan zonder toestemming van het systeembeheer.
- Het aansluiten van eigen apparatuur (zoals laptops, tablets en telefoons) is alleen toegestaan op de daarvoor beschikbaar gestelde (draadloze) netwerkaansluitingen. Het systeembeheer kan aan de toegang tot deze aansluitingen regels verbinden ter handhaving van deze gedragscode, zoals het moeten installeren van virusscanners en wachtwoordbeveiliging.

5.1. Werkplek

Voorkom dat anderen (onbedoeld) toegang kunnen krijgen tot bedrijfsmiddelen waartoe zij geen rechten hebben en/of laat gegevens niet (onbedoeld) lekken. Als aanvullende regels op computergebruik gelden voor de werkplek de volgende clean desk en clear screen regels:

- Vergrendel bij het tijdelijk verlaten van de werkplek de pc (windowstoets+L).
- Verwijder interne en vertrouwelijke documenten van het bureau bij het voor langere tijd verlaten van de werkplek (denk hieraan bij het bijwonen van een vergadering).
- Voorkom dat gevoelige en vertrouwelijke informatie zichtbaar is wanneer iemand anders op het beeldscherm (of via een beamer) mee kan kijken. Sluit het e-mailprogramma af en zorg voor een opgeruimd digitaal bureaublad.
- Laat geen afdrukken bij de printer liggen, zeker niet als er persoonsgegevens op staan.
- Haal overbodig geworden papieren documenten met persoonsgegevens erop altijd door de papierversnipperaar.

LET OP: Als persoonsgegevens toegankelijk/inzichtelijk zijn voor personen, die geen toegang behoren te hebben tot die gegevens is er sprake van een beveiligingsincident, waaruit mogelijk een datalek kan voortkomen. Weet dat beveiligingsincidenten en mogelijke datalekken gemeld moeten worden volgens de procedure Datalekken en de meldplicht van de stichting Ubbo Emmius.

5.2. Gebruik eigen devices (BYOD)

Beveiligingsmaatregelen hebben betrekking op alle devices waarmee werkzaamheden voor de school worden uitgevoerd. De stichting Ubbo Emmius is verantwoordelijk voor het implementeren van de juiste beveiligingsmaatregelen als het gaat om de bedrijfsmiddelen van de school.

Voor ‘Own Devices’ ligt de verantwoordelijkheid voor adequate beveiligingsmaatregelen bij de medewerker zelf. Van de medewerker wordt verwacht dat minimaal de volgende beveiligingsmaatregelen worden genomen:

- Beveilig het device met een wachtwoord, of in het geval van een smartphone of tablet, met een pincode die langer is dan 4 tekens.
- Vergrendel het device bij het verlaten van de werkplek (windowstoets+L).
- Sla *persoonsgegevens* van de stichting Ubbo Emmius niet op het eigen device op; dit is niet toegestaan.
- Versleutel alle gegevens, anders dan persoonsgegevens, met betrekking tot de stichting Ubbo Emmius als deze, om welke reden dan ook, niet op het schoolnetwerk opgeslagen worden (denk hierbij aan het eigen device of usb-stick).
- Scheid (versleutelde)gegevens, anders dan persoonsgegevens, van de stichting Ubbo Emmius en privégegevens van elkaar. Deze scheiding moet duidelijk herkenbaar zijn op het eigen device.
- Houd software up-to-date door het uitvoeren van periodieke updates (minimaal maandelijks).
- Neem adequate maatregelen tegen virussen of malware door het up-to-date houden van de virusscanner en door het periodiek (minimaal maandelijks) scannen van het device.

De stichting Ubbo Emmius mag controles uitvoeren op bovenstaande maatregelen. Op verzoek van de stichting Ubbo Emmius moet de medewerker zelf aantonen dat de bovenstaande maatregelen worden toegepast.

5.3. Software en digitaal lesmateriaal

Het gebruik van digitaal lesmateriaal is niet meer weg te denken bij de stichting Ubbo Emmius. Dit lesmateriaal staat steeds meer online waarbij steeds vaker persoonsgegevens worden uitgewisseld. De privacywetgeving eist dat elke organisatie vooraf aan het gebruik van dergelijk materiaal bekijkt wat de invloed ervan is op de privacy, dit kan specifieke maatregelen tot gevolg hebben.

De onderstaande regels gelden voor installatie en gebruik van software en (online)digitaal lesmateriaal:

- Installeren van software wordt bij de stichting Ubbo Emmius alleen toegestaan met de juiste licenties en na het nemen van eventuele aanvullende maatregelen.
- Bij het gebruik van onlinesoftware, app's en digitaal lesmateriaal, wordt gekeken of er persoonsgegevens bij verwerkt worden.
- Een verwerkersovereenkomst wordt afgesloten met elke leverancier van (online)software, die in opdracht van de stichting Ubbo Emmius persoonsgegevens verwerkt. Regel dit vooraf aan het gebruik.
- Aanvragen van digitaal lesmateriaal en/of andere software volgt bij de stichting Ubbo Emmius de afgesproken aanvraagprocedure. Aanvragen moeten worden ingediend bij het hoofd systeembeheer die vervolgens onderzoekt welke eventuele wettelijk verplichte aanvullende privacy- en/of beveiligingsmaatregelen nodig zijn.

6. Gebruik van e-mail en andere ict-communicatiemiddelen

Het e-mailsysteem en de bijbehorende mailbox en e-mailadres worden aan de leerlingen en werknemers beschikbaar gesteld. Gebruik is verbonden aan taken die voortvloeien uit deze functie. Het is verboden de ICT-communicatiemiddelen te gebruiken voor:

- het verzenden van berichten met een pornografische, racistische, discriminerende, bedreigende, (seksueel) intimiderende, beledigende of aanstootgevende inhoud;
- het versturen van ongevraagde berichten aan grote aantallen ontvangers, kettingbrieven te versturen of kwaadaardige software zoals virussen, Trojaanse paarden of spyware te versturen.

Gebruik het school-e-mailadres *uitsluitend* voor schoolgerelateerde zaken. Gebruik voor privé e-mail een eigen privé e-mailadres via een externe webmaildienst (bijvoorbeeld webmail van Gmail, Hotmail of een eigen provider). Ontvangen van privémail op het school e-mailadres is incidenteel toegestaan. Het versturen van e-mail moet voldoen aan de normale gedragsregels die gelden voor schriftelijke correspondentie.

Synchroniseert een medewerker de school e-mail met een eigen device (tablet, telefoon) dan kan de stichting Ubbo Emmius, bij verlies of diefstal van het device, gebruik maken van de mogelijkheid om de e-mail op afstand te wissen, ook als daarmee alle (privé)gegevens van het device gewist worden.

In geval van ziekte, onverwacht langdurige afwezigheid of grove nalatigheid van de leerling of werknemer, doch uitsluitend als dit een zwaarwegende reden van bedrijfsbelang tot toegang oplevert, is de stichting Ubbo Emmius gerechtigd om, bij de afdeling ICT, toegang tot de bestanden of mailbox van de leerling of werknemer aan te vragen. In het geval van ziekte of onverwacht langdurige afwezigheid is hiervoor aparte toestemming nodig van een van de stafdirecteuren. Bij grove nalatigheid is aparte toestemming van het CvB vereist.

Ubbo Emmius mag zich echter geen toegang verschaffen tot als privé gemarkeerde mappen, als privé herkenbare mails, of e-mails verzonden naar dan wel afkomstig van een vertrouwenspersoon. Indien de leerling of werknemer dergelijke markeringen niet heeft aangebracht, kan Ubbo Emmius door inschakeling van een vertrouwenspersoon de betreffende informatie van de leerling of werknemer controleren om zo privéinformatie te herkennen en apart te plaatsen alvorens er toegang kan zijn.

E-mailberichten van leden van het medezeggenschapsorgaan onderling, van bedrijfsartsen, van HR-/P&O-adviseurs en van eenieder 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.

7. Gebruik van internet

De toegang tot internet en bijbehorende faciliteiten worden aan leerlingen, (tijdelijke)werknemers, zelfstandige adviseurs en bezoekers beschikbaar gesteld. Gebruik hiervan is verbonden aan deze werkzaamheden en gaat uit van de volgende afspraken:

- Beperkt persoonlijk gebruik is toegestaan, mits dit
  - niet storend is voor de dagelijkse werkzaamheden;
  - niet voor commerciële doeleinden is en
  - geen verboden gebruik oplevert.

- Het is daarbij verboden:
  - sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten;
  - films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van enige illegale bron;
  - films, muziek, software en overig auteursrechtelijk beschermd materiaal te verspreiden (uploaden) naar derden zonder toestemming van de rechthebbenden;

- onder lestijd internettoegang te gebruiken voor privédoeleinden;
- deel te nemen aan kansspelen.

Het is verboden op dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende toon te communiceren via online fora, sociale netwerken en andere vergelijkbare communicatienetwerken over alle aan school verbonden betrokkenen en activiteiten. Dit geldt in het bijzonder ook voor internetgebruik buiten het schoolnetwerk met betrekking tot aan de school verbonden betrokkenen en activiteiten.

Voor toegestane activiteiten geldt een 'fair use policy', waarbij systeem- en netwerkbeheerders de mogelijkheid hebben om in te grijpen wanneer activiteiten leiden tot overlast bij andere gebruikers.

7.1. Veilig online

We brengen met z'n allen steeds meer tijd online door. Hierbij worden steeds meer mobiele devices gebruikt. Menselijk (online)handelen staat veelal aan de basis van een datalek.

De stichting Ubbo Emmius verwacht van medewerkers dat zij:

- het onderscheid kennen tussen veilige en onveilige netwerken (openbare wifinetwerken) en websites;
- bij het verwerken van persoonsgegevens alléén gebruik maken van bekende én beveiligde draadloze netwerken;
- weten wat malware is, het kunnen herkennen en weten hoe te handelen;
- terughoudend zijn met het online achterlaten van gegevens met betrekking tot de stichting Ubbo Emmius;
- controleren of er daadwerkelijk van een bekend én beveiligd netwerk gebruik gemaakt wordt bij het bezoek aan openbare ruimtes. (Een netwerk kan bekend zijn omdat het een Ubbo Emmius-netwerk is, eduroam of het eigen draadloze netwerk thuis is).

7.2. Sociale media

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

Voor gebruik van sociale media geldt als uitgangspunt dat het digitale gedrag op sociale media niet afwijkt van het real life gedrag binnen de school. Medewerkers zijn altijd de vertegenwoordiger van de stichting Ubbo Emmius ook als zij online een privémening verkondigen.

Bij de stichting Ubbo Emmius gelden de volgende afspraken voor het gebruik van sociale media:

- Deel op verantwoorde wijze kennis via sociale media rekening houdend met de goede naam van de stichting Ubbo Emmius en iedereen die hierbij betrokken is.
- Maak bij onderwijs gerelateerde onderwerpen duidelijk of publicatie op persoonlijke titel of namens de stichting Ubbo Emmius gedaan wordt.
- Publiceer geen vertrouwelijke informatie op sociale media.
- Publiceer geen beeldmateriaal van leerlingen zonder de uitdrukkelijke voorafgaande aantoonbare toestemming van ouders als de leerling jonger is dan 16 jaar of de leerling zelf als deze ouder is dan 16 jaar.
- Weet dat publicaties op sociale media altijd vindbaar (openbaar) en moeilijk vernietigbaar zijn.
- Medewerkers zijn persoonlijk verantwoordelijk voor wat zij publiceren.
- Neem contact op met een leidinggevende als er twijfel bestaat over een publicatie of over de raakvlakken met de stichting Ubbo Emmius.
- Het is medewerkers niet toegestaan om met een privéaccount ‘vrienden’ te worden met leerlingen en ouders op sociale media.
- Inzetten van sociale media in het lesprogramma is gebonden aan de toestemming van ouders als leerlingen jonger zijn dan 16 jaar.

Aanvullende afspraken rondom social media in het algemeen heeft de stichting Ubbo Emmius vastgelegd in een apart Protocol Sociale Media, dat te vinden is op het UbboNet.

7.3. Gebruik beeld- en geluidsmateriaal

Het gebruiken van beeld- en geluidsmateriaal, het delen van foto's, video's en geluidsfragmenten van leerlingen door medewerkers vallend onder de stichting Ubbo Emmius mag alleen, als daar vooraf toestemming voor gegeven is door ouders als de leerling jonger is dan 16 jaar of de leerling zelf als deze ouder dan 16 jaar is. Zonder deze toestemming mogen *geen* foto's, video's en geluidsfragmenten van leerlingen gebruikt worden.

De stichting Ubbo Emmius verwijst hierbij naar de richtlijn die is opgesteld in het protocol Publicatie Beelmateriaal.

Voor de afspraken rondom het delen van beeld- en geluidsmateriaal via sociale media gelden de richtlijnen die genoemd worden bij het gebruik van sociale media.

7.4. Wachtwoorden en pincodes

Het beveiligen van toegang tot het netwerk, diverse (online) applicaties en devices (pc, laptop, telefoon) begint met een goed wachtwoord. Een lang wachtwoord of een 'wachtzin' is beter dan een kort, complex wachtwoord. Voor het gebruik van wachtwoorden gelden onderstaande afspraken:

- Wachtwoorden moeten minimaal 8 tekens bevatten, met minstens drie van de volgende vier elementen: kleine letter, hoofdletter, cijfer of speciaal teken (!@#$%^&*()
- Pincodes (op telefoon of tablet) moeten langer zijn dan 4 tekens.

- Wachtwoorden moeten volgens de afspraken binnen de stichting Ubbo Emmius op aangegeven tijden vervangen worden.
- Gebruik niet voor elke systeem hetzelfde wachtwoord.
- Deel wachtwoorden nooit, ook niet incidenteel. Wachtwoorden zijn persoonlijk.

7.5. Meldplicht Datalekken

Van alle medewerkers wordt verwacht dat zij beveiligingsincidenten en mogelijke datalekken melden volgens de procedure Datalekken van de stichting Ubbo Emmius.

8. Monitoring en controle

De stichting Ubbo Emmius handelt bij de controle op het gebruik van bedrijfsmiddelen binnen de geldende wet- en regelgeving, te weten:

- De Grondwet,
- Wet bescherming persoonsgegevens (Wbp; tot 25 mei 2018),
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)
- Wet Medezeggenschap Onderwijs (WMO)
- Burgerlijk Wetboek (BW)
- Wetboek van Strafrecht en de
- Cao VO.

De stichting Ubbo Emmius zal bij controle rondom het gebruik van bedrijfsmiddelen op basis van deze gedragscode uitgaan van de juiste balans tussen verantwoord gebruik van bedrijfsmiddelen en de bescherming van de privacy van medewerkers.

8.1. Voorwaarden voor controle

- Controle van persoonsgegevens met betrekking tot gebruik van bedrijfsmiddelen vindt slechts plaats in het kader van handhaving van de doelen van deze gedragscode.
- Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot identificeerbare personen.
- Indien een medewerker of een groep medewerkers wordt verdacht van het overtreden van regels, kan gedurende een vastgestelde (korte) periode, in opdracht van de stichting Ubbo Emmius gerichte controle plaatsvinden.

- Controle beperkt zich in beginsel tot verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen vindt, in opdracht van de stichting Ubbo Emmius, controle op de inhoud plaats.
- Verboden e-mail- en internetgebruik wordt zo veel mogelijk softwarematig onmogelijk gemaakt.
- Bij constatering van ongeoorloofd gebruik wordt dit onmiddellijk met de betrokken medewerker besproken. De stichting Ubbo Emmius zal de medewerker op verzoek inzage verschaffen in de gegevens over het eigen gebruik. De medewerker wordt gewezen op de consequenties wanneer niet wordt gestopt met het ongeoorloofd gebruik.
- E-mailberichten van leden van de GMR onderling, van vertrouwenspersonen, bedrijfsartsen en van eenieder die zich op grond van zijn functie op enige vertrouwelijkheid moet kunnen beroepen, worden in principe niet gecontroleerd. Dit geldt niet voor veiligheid van berichten. Ook hier kan bij zwaarwegende redenen van afgeweken worden.

8.2. Uitvoering van de controle

- De controle ter voorkoming van negatieve publiciteit en seksuele intimidatie en de controle in het kader van systeem- en netwerkbeveiliging vindt plaats op basis van content-filtering.
- De controle op het uitlekken van interne en vertrouwelijke gegevens vindt plaats op basis van steekproefsgewijze content-filtering. Verdachte berichten worden apart gezet voor nader onderzoek.
- De controle in het kader van kosten- en capaciteitsbeheersing wordt beperkt tot verkeers- en opslaggegevens.
- Controle op het gebruik van beeldmateriaal vindt plaats op basis van klachten of meldingen van derden, of steekproefsgewijs bij beeldmateriaal dat openbaar beschikbaar is.
- De afdeling ICT, de systeembeheerder(s) zijn aan geheimhouding gebonden als men om technische redenen kennis moet nemen van persoonsgebonden informatie, behalve als enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.
- Door de stichting Ubbo Emmius worden de nodige maatregelen getroffen, opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn.
- Door de stichting Ubbo Emmius worden passende technische en organisatorische maatregelen getroffen om persoonsgegevens te beveiligen tegen verlies en/of tegen enige vorm van onrechtmatige verwerking.

8.3. Disciplinaire maatregelen

Bij het handelen in strijd met deze gedragscode of de algemeen geldende wettelijke regels, kan het bestuur van de stichting Ubbo Emmius, afhankelijk van de aard en de ernst van de overtreding, disciplinaire maatregelen treffen. Hieronder vallen o.a. een waarschuwing/berisping, schadevergoeding, aangifte bij de politie, overplaatsing, schorsing en/of beëindiging van de arbeidsovereenkomst.

Medewerkers die zich niet aan deze gedragscode houden, worden zo spoedig mogelijk door de leidinggevende op hun gedrag aangesproken. Zij krijgen daarbij inzage in de over hen vastgelegde

gegevens en hebben de gelegenheid te reageren op het geconstateerde. Medewerker en leidinggevende maken dan afspraken voor de toekomst en bepalen de mogelijke maatregelen bij overtreding daarvan. Deze afspraken kunnen strenger zijn dan het in deze gedragscode bepaalde. Ook kan de toegang tot e-mail of internet worden beperkt of geheel worden afgesloten. Disciplinaire maatregelen (behalve een waarschuwing) kunnen niet enkel op basis van een langs geautomatiseerde uitgevoerde verwerking van persoonsgegevens worden getroffen, zoals een constatering van een automatisch filter of blokkade. Er worden geen disciplinaire maatregelen getroffen zonder dat de medewerker gelegenheid heeft gekregen zijn zienswijze naar voren te brengen.

8.4. Bezwaar en beroep

Als de medewerker het niet eens is met de (voorgenomen) disciplinaire maatregel, dan kan daar in een aantal gevallen bezwaar en/of beroep tegen worden ingesteld. Dit is meestal geregeld in de arbeidsovereenkomst, regels rondom personeelszaken en/of de van toepassing zijnde cao.

9. Slotbepaling

Deze gedragscode wordt jaarlijks geëvalueerd door het CvB, de manager IBP en de Functionaris Gegevensbescherming. Deze gedragscode kan, na instemming van de medezeggenschapsorganen, worden gewijzigd als de omstandigheden daar aanleiding toe geven. Voorgenomen wijzigingen worden voorafgaand aan de invoering aan de leerlingen, studenten en werknemers bekend gemaakt.

In gevallen waarin deze gedragscode niet voorziet, beslist het CvB.