Gedragscode informatiebeveiliging voor medewerkers[1]

Versie: schooljaar 2020/2021.
Auteurs: Joris Weel (Security Officer), Jan van den Hazelkamp (Coördinator IPB) en Carol van Lent (Functionaris Gegevensbescherming).
Onderdeel van het IBP beleid van Curio.

Dit reglement vervangt de versie 2019 en treedt in werking na vaststelling door de Raad van Bestuur en na instemming door de aangewezen organen.

17-11-2020	De Raad van Bestuur stelt de herziene versie van het Informatie- en privacybeleid inclusief bijlagen vast voor Curio ,met instemming van de Studentenraad, de Ondernemingsraad en de Ouderraad vmbo scholen.

Inhoud

[1] Exclusief Graaf Engelbrecht en Stedelijk Gymnasium Breda.

1. Inleiding

1.1 Aanleiding

Het gebruik van ICT is voor de medewerkers noodzakelijk om het werk goed te kunnen doen.
Het gebruik van Social Media kan ook zijn weerslag hebben op Curio. Daarnaast wordt er met vertrouwelijke (persoons)gegevens gewerkt. Een goede inrichting van de werkplek is daarbij van belang om inbreuk op de privacy (datalekken) te voorkomen.
Curio is als werkgever bevoegd regels te stellen omtrent de uitvoering van het werk en de goede orde op de werkvloer.

1.2 Scope

Deze gedragscode stelt regels aan:

- Het gebruik van ICT-faciliteiten van Curio;
- Het gebruik van (privé) ICT-middelen waarmee de medewerker is aangesloten op het computernetwerk van Curio;
- ICT middelen waarop je gegevens van Curio verwerkt;
- Het gebruik van Social Media namens Curio;
- De inrichting van de werkplek waarbinnen je ICT-middelen en gegevens van Curio gebruikt;
- Regels met betrekking tot werk op afstand (telewerken).

Deze gedragscode geeft daarnaast voorschriften over de wijze waarop toezicht op en onderzoek naar de naleving ervan plaats vindt.

1.3 Doel

Doel van deze regels en voorschriften is de goede orde te bepalen ten aanzien van onder andere:

- Bescherming van (privacy gevoelige) gegevens van Curio en haar medewerkers;
- Bescherming van vertrouwelijke informatie van Curio en haar medewerkers;
- Bescherming van de intellectuele eigendomsrechten van Curio en derden waaronder het respecteren van de licentie-afspraken die van toepassing zijn binnen Curio;
- Tegengaan van (seksuele) intimidatie, discriminatie en andere strafbare feiten;
- Voorkomen van negatieve publiciteit;
- Voorkomen van schade aan en misbruik van ICT-middelen.

1.4 Reikwijdte

Dit Reglement geldt voor eenieder die voor Curio werkzaam is, dus ook voor uitzendkrachten en tijdelijke medewerkers. Dit Reglement kan door Curio worden herzien. Wijzigingen worden alleen bij het begin van een collegejaar doorgevoerd, behalve in dringende gevallen of wanneer Curio door omstandigheden van buitenaf gedwongen is tot een snellere invoering.

2. Reglement

2.1 Gebruik van computernetwerk account

2.1.1 Toelichting

De medewerker krijgt een account, waarmee toegang tot het computernetwerk kan worden verkregen. Degene aan wie de accounts zijn verstrekt, is verplicht al hetgeen te doen dan wel na te laten wat redelijkerwijs van hem/haar mag worden verwacht om misbruik van de verstrekte accounts te voorkomen

2.1.2 Uitgangspunten

- De medewerker dient te allen tijde zorgvuldig om te gaan met aan hem persoonlijk toegekende inloggegevens en aanvullende authenticatiemiddelen (zoals bijvoorbeeld smartcards en tokens).
- De door Curio aan medewerkers verleende accounts zijn strikt persoonlijk;
- Persoonsgebonden wachtwoorden en aanvullende authenticatiemiddelen mogen niet worden gedeeld;
- Indien door nalatigheid, hetzij door opzet van de gebruiker systemen of het netwerk (deels) wordt platgelegd of hieraan op andere wijze schade wordt veroorzaakt zal de gebruiker het gebruik van deze voorzieningen worden ontzegd;
- Schade en kosten kunnen door Curio op de gebruiker worden verhaald;
- In gevallen waarin dit Reglement niet voorziet, beslist de Raad van Bestuur.

2.2 Gebruik van faciliteiten

2.2.1 Toelichting

ICT-faciliteiten, zoals (openbare) computers, draadloze en bedrade netwerkaansluitingen, e-mail, internettoegang, opslagcapaciteit, printers en elektronische werkomgevingen worden aan de medewerker beschikbaar gesteld om werkzaamheden voor Curio uit te voeren.
Het gebruik van eigen apparatuur en toepassingen is toegestaan zolang dit gebruik voldoet aan de regels van dit Reglement.

2.2.2 Uitgangspunten

- ICT-faciliteiten 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;
- Beperkt privégebruik van internet en ICT-middelen is alleen toegestaan tijdens pauzes en/of voor zover het werk er niet onder lijdt;
- 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;
- Het veranderen van instellingen in apparatuur en toepassingen beschikbaar gesteld door Curio is alleen toegestaan met aparte toestemming van de ICT-beheerder;
- 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;
- De maker dan wel verzender van een elektronisch bericht vermeldt altijd zijn volledige naam en een onderwerp waarover het bericht gaat;
- Het is absoluut niet toegestaan internetsites te bezoeken, bestanden op het schoolnetwerk te plaatsen, of e-mailberichten te verzenden die godslasterlijk, pornografisch, racistisch of anderszins discriminerend materiaal bevatten;
- Opslag en verwerking van onrechtmatig verkregen informatie of informatie waarvan het bezit strafbaar is, zijn niet toegestaan, ook niet voor privédoeleinden;
- Het gebruik van computer, e-mail en internet mag geen onevenredige belasting vormen voor de IT-infrastructuur van Curio;
- Het is niet toegestaan software te gebruiken welke niet door Curio is aangeleverd of waarvoor vooraf geen schriftelijke toestemming tot gebruik is verkregen;
- Het installeren van software op de computer- en netwerkfaciliteiten van de organisatie is niet toegestaan zonder aparte toestemming van de IT-afdeling;

- Het is niet toegestaan handelingen te verrichten welke gericht zijn op het aanmaken, binnenhalen, en/of verspreiden van virussen in welke vorm dan ook, almede handelingen te verrichten welke gericht zijn op het ongewenst benaderen en/of binnendringen van computers en computersystemen (hacken);

2.3 Gebruik van Social Media

2.3.1 Toelichting

Curio 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).

2.3.2 Uitgangspunten

- Indien dit werk gerelateerde onderwerpen betreft, dient de medewerker altijd de naam van Curio 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 Curio;
- Bestuurders, managers, leidinggevenden en anderen die namens Curio 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;
- 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;
- Wanneer medewerker een sociale-media-account opzet dat direct werk gerelateerd is, terwijl het op naam van medewerker persoonlijk is gesteld, zullen medewerker en Curio bij beëindiging van het dienstverband een passende oplossing zoeken voor het overdragen van dit profiel of de informatie en contacten.

2.4 Werken op afstand (beeldbellen)

2.4.1 Toelichting

We werken steeds meer op afstand. We geven les op afstand en volgen vergaderingen online. Deze manier van werken heeft impact op de privacy van de medewerker. Daarnaast heeft het impact op de wijze waarop we met elkaar omgaan.

2.4.2 Uitgangspunten

- Zorg ervoor dat er geen privacygevoelige gegevens of andere personen ongewenst in beeld komen, zodra de camera aan staat.
- Bij voorkeur wordt de achtergrond vervaagt, middels de opties die de applicatie daarvoor biedt (blur functie).
- Bij voorkeur wordt er een headset of koptelefoon gebruikt.
- Bij voorkeur wordt de microfoon gedempt. Als de microfoon aan staat, zorgt de spreker ervoor dat er geen privégesprekken of andere storende geluiden hoorbaar zijn.
- Bij voorkeur worden gesprekken niet opgenomen. Mocht dit toch nodig zijn dan dienen de gesprekdeelnemers te worden geïnformeerd over het doel en bewaartermijn van de opname. Deze opnames mogen niet openbaar gepubliceerd worden, niet met onbevoegden gedeeld worden en dienen na de afgesproken bewaartermijn verwijderd te worden.

2.5 Les op afstand

2.5.1 Toelichting

Er zijn verschillende manieren om les op afstand te geven. Deze verschillende manieren hebben ook ieder een eigen impact op de privacy van zowel de student als de docent. Dit document geeft de richtlijnen aan voor het geven van les op afstand zoals Curio deze hanteert.

2.5.2 Algemene richtlijnen

- Zorg ervoor dat er geen privacygevoelige gegevens of andere personen ongewenst in beeld komen, zodra de camera aan staat.
- Bij voorkeur wordt de achtergrond vervaagt, middels de opties die de applicatie daarvoor biedt (blur functie).
- Bij voorkeur wordt er een headset of koptelefoon gebruikt.

- Bij voorkeur wordt de microfoon gedempt. Als de microfoon aan staat, zorgt de spreker ervoor dat er geen privégesprekken of andere storende geluiden hoorbaar zijn.

2.5.3 Voor studenten geldt:

- De studenten die thuis de les volgen, zijn niet verplicht gedurende de hele les de camera aan te zetten. Echter mag er van de studenten worden verwacht dat zij in beeld komen op de momenten dat de docent dit noodzakelijk acht.
- Studenten mogen de les niet opnemen en ook niet filmen.
- Studenten mogen geen foto's of screenshots van de les maken.

2.5.4 Voor docenten geldt:

- Docenten zijn niet verplicht om zichzelf in beeld te brengen, tenzij dit in het kader van het geven van onderwijs nodig is.
- Bij voorkeur worden de lessen niet opgenomen. Mocht dit toch nodig zijn, dan dienen de studenten te worden geïnformeerd over het doel en bewaartermijn van de opname. Deze opnames mogen niet openbaar gepubliceerd worden, niet met onbevoegden gedeeld worden en dienen na de afgesproken bewaartermijn verwijderd te worden.

Aanvullende richtlijnen bij het streamen van een les vanuit een locatie met studenten:

- Zorg ervoor dat de studenten die in de klas aanwezig zijn onherkenbaar in beeld zijn. Hang de camera bij voorkeur achter in de klas. Op die manier zijn gezichten niet zichtbaar in beeld.

2.6 Intellectueel eigendom en vertrouwelijke informatie

2.6.1 Toelichting

De medewerker maakt geen inbreuk op de intellectuele eigendomsrechten van Curio en derden en respecteert de licentieafspraken zoals die van toepassing zijn binnen Curio.
Curio 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 ("need to know" principe).

2.6.2 Uitgangspunten

- De zeggenschap over de informatie van Curio berust bij Curio. De medewerker heeft geen zelfstandige zeggenschap over de informatie behalve als hem dat expliciet is toegekend;
- Indien de medewerker in het kader van zijn werkzaamheden of het uitvoeren van taken voor Curio toegang krijgt tot vertrouwelijke informatie of privacy gevoelige informatie waaronder persoonsgegevens, dient de medewerker die informatie strikt vertrouwelijk te behandelen;
- Indien Curio met betrekking tot het waarborgen van de vertrouwelijkheid en de intellectuele eigendomsrechten voorschriften heeft opgesteld, dient de medewerker deze stipt op te volgen. De medewerker maakt geen inbreuk op de intellectuele eigendomsrechten van Curio en derden en respecteert licentieafspraken zoals die van toepassing zijn binnen Curio.
- 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.
- Het is uitdrukkelijk niet de bedoeling dat instellingsgebonden vertrouwelijke informatie opgeslagen of verwerkt wordt:
    - Binnen niet instellingsgebonden Cloud-toepassingen;
    - Op externe opslagmedia of eigen cliëntapparatuur (USB-apparaten, Tablets, etc.).

  Mocht dit toch noodzakelijk zijn dan:
    - Gebeurt dit alleen met goedkeuring van de Functionaris Gegevensbescherming;
    - Besteedt de medewerker bijzondere aandacht aan het treffen van maatregelen zoals in dit Reglement genoemd.

2.7 Beveiliging door Curio én de medewerker

2.7.1 Toelichting

Curio neemt informatiebeveiliging serieus. Curio 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 100% beveiliging onmogelijk. Daarom verwacht Curio ook van medewerkers een proactieve houding en serieuze stappen om de eigen computer en andere apparatuur (zoals smartphones of tablets) adequaat te beveiligen. Zo is de medewerker te allen tijde zelf verantwoordelijk voor het gebruik van de eigen apparatuur en de op deze apparatuur opgeslagen gegevens.

2.7.2 Uitgangspunten

Wanneer gebruik wordt gemaakt van privé apparatuur, verwachten we in het kader van beveiliging:

- Dat de apparatuur is voorzien van een adequate virusscanner en firewall;
- De eigenaar regelmatig reserve kopieën maakt van alle relevante data;
- Kopieën van data veilig opgeslagen worden;
- Moeilijk te raden wachtwoorden worden gebruikt en deze regelmatig worden veranderd;
- De apparatuur up-to-date wordt gehouden wat betreft software-instellingen.

2.8 Gebruik en overlast

2.8.1 Toelichting

Beperkt privégebruik van de faciliteiten is toegestaan.

2.8.2 Uitgangspunten

- Gebruik, privé of voor werk, mag niet storend zijn voor de goede orde bij Curio en mag geen overlast veroorzaken bij anderen, inbreuk maken op rechten van Curio 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 Uitzending gemist) 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;
  - Films, muziek, software en overig auteursrechtelijk beschermd materiaal te verspreiden (uploaden) naar derden zonder toestemming van de rechthebbenden.

- Verder is het niet toegestaan:
  - Eigen netwerkapparatuur zoals bijvoorbeeld servers, networked attached storage, access points en routers aan te sluiten.

- Wat mag wel, wanneer het niet verstorend is en voldoet aan de eerder genoemde eisen:
  - 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 mobile device management (MDM), certificaten, virusscanners en eisen stellen aan de beveiligingsinstellingen, zoals bijvoorbeeld wachtwoordvereisten.
  - Het beperkt opslaan van privébestanden of -informatie op systemen van Curio:
    - Mits dit niet leidt tot overbelasting van de opslagcapaciteit van de systemen;
    - Het niet leidt tot verstoring van de goede orde op de werkvloer

    Curio is niet verplicht van dergelijke bestanden of informatie reservekopieën te maken of kopieën beschikbaar te stellen bij vervanging of reparatie van de betreffende systemen. Ook kan de organisatie je verzoeken de gegevens te verwijderen, wanneer dit niet binnen de afgesproken termijn gebeurt, is het Curio toegestaan de gegevens zonder toestemming te verwijderen.
  - De organisatie zal de toegang tot openbare e-maildiensten (gmail, hotmail etc.) niet blokkeren of specifiek monitoren. De medewerker gebruikt het door Curio verstrekte

e-mail adres daarom bij voorkeur niet voor privémail. Mochten er toch privé e-mails worden ontvangen en opgeslagen binnen de zakelijke e-mail, dan moet hiervoor een apart opslagarchief “privé” worden aangemaakt waarin deze berichten worden bewaard.

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

2.9 Monitoring door Curio

2.9.1 Toelichting

Behoudens wettelijke uitzonderingen, vindt controle van gebruik van de faciliteiten slechts plaats in het kader van handhaving van de regels uit dit Reglement ten behoeve van de goede orde binnen Curio en de bewaking van de integriteit en de veiligheid van het netwerk en de computerfaciliteiten van Curio. Verboden gebruik van de faciliteiten wordt zo veel mogelijk langs technische weg onmogelijk gemaakt.

2.9.2 Uitgangspunten

- 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 medewerkers, worden overgegaan tot uitschakeling van de netwerktoegangsmogelijkheden. Indien mogelijk wordt de medewerker 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) of unit directeur (VMBO) 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.
- Curio houdt zich bij het controleren op het niveau van verkeersgegevens of de inhoud onverkort aan de AVG en andere relevante regelgeving. In het bijzonder beveiligt Curio de bij controle vastgelegde gegevens tegen ongeautoriseerde toegang en worden personen met toegang daartoe contractueel verplicht tot geheimhouding.
- Enkele specifieke maatregelen ter controle die Curio 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.
- Algemeen toezicht door een daartoe aangewezen functionaris van de dienst ICT en de andere ICT- eenheden heeft als doel systeem- en netwerkbeveiliging te waarborgen. Algemeen toezicht houdt in het zorgdragen dat onbevoegden geen toegang krijgen tot (persoons)gegevens, systemen en netwerken;
- ICT-functionarissen hebben geheimhoudingsplicht met betrekking tot gegevens over e-mail en internetgebruik die tot personen herleidbaar zijn.
- ICT-functionarissen nemen zodanige maatregelen dat een passend beveiligingsniveau wordt bereikt gelet op de risico’s die de verwerking en de aard van de te beschermen gegevens met zich meebrengen;
- Verkeersgegevens (gegevens over afzender, bestemming, datum en tijd) over e-mail- en internetgebruik worden in beginsel niet langer bewaard dan zes maanden. In geval van een

vermoeden van onjuist gebruik kunnen deze gegevens langer worden bewaard totdat de noodzaak daartoe is vervallen;
- Bij een vermoeden van onjuist gebruik wordt de betreffende medewerker zo spoedig mogelijk op zijn/haar gedrag aangesproken.
- Zaken die niet op Curio systemen en PC's thuishoren zoals eigen en/of illegale software, films en muziek, worden na overleg met de betrokken direct leidinggevende verwijderd. De medewerker wordt hierover vooraf geïnformeerd tenzij het onderzoek daardoor wordt belemmerd;

2.10 Procedure bij gericht onderzoek

2.10.1 Toelichting

Van gericht onderzoek is sprake wanneer verkeersgegevens of andere persoonsgegevens van de medewerker worden vastgelegd in het kader van een onderzoek naar aanleiding van een redelijke verdenking van een overtreding van dit Reglement door die medewerker, dan wel andere misdragingen.

2.10.2 Uitgangspunten

- Gericht onderzoek vindt slechts plaats naar aanleiding van gerechtvaardigde vermoedens dan wel constatering van onjuist gebruik.
- Enkele specifieke persoonsgebonden maatregelen ter controle die Curio 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 na overleg met de Raad van Bestuur;
    - controle op overtreding van het Reglement vindt plaats door twee personen naar aanleiding van een klacht, redelijke verdenking of steekproefsgewijs door E mailberichten te openen en de inhoud te raadplegen. Deze personen zijn gebonden aan geheimhouding over de inhoud en zullen hun bevindingen slechts aan de directie dan wel de Raad van Bestuur doorgeven.
- Gericht onderzoek vindt uitsluitend plaats na schriftelijke opdracht van de directeur van de organisatie-eenheid waaronder de medewerker valt, waarbij de reden vermeld zal worden waarom tot dit gerichte onderzoek zal worden overgegaan.
- De medewerker te wiens laste een onderzoek plaatsvindt, wordt zo spoedig mogelijk schriftelijk geïnformeerd over de aanleiding, de uitvoering en het resultaat van het onderzoek. Het verstrekken van informatie aan de medewerker wordt uitgesteld indien het onderzoek daardoor wordt geschaad;
- Indien er sprake is van een redelijke verdenking van een overtreding van dit reglement of een andere misdraging is, dan wel het vermoeden bestaat dat een medewerker zich schuldig maakt aan een strafbaar feit, kan er ook een heimelijke controle plaatsvinden. In dat geval zal de medewerker pas achteraf, na afronding van het onderzoek, over de heimelijke controle worden geïnformeerd.
- De portefeuillehouder van de Raad van Bestuur ontvangt een afschrift van deze opdracht en een schriftelijk verslag 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 (namens) Curio na voorafgaande aparte toestemming van de Raad van Bestuur hiervoor, worden overgegaan tot het kennisnemen van de inhoud van communicatie of opgeslagen bestanden. De medewerker wordt in de gelegenheid gesteld uitleg te geven over de aangetroffen gegevens.
- 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 medewerker met het doel de beveiliging of integriteit van de randapparatuur te verbeteren.

2.10.3 Bezwaar

De medewerker ten aanzien van wie gericht onderzoek is of wordt uitgevoerd kan daartegen schriftelijk en gemotiveerd bezwaar aantekenen binnen vier weken nadat de medewerker is ingelicht over het onderzoek.

- Een ingediend bezwaar schort getroffen of te treffen maatregelen niet op;

- De algemeen directeur reageert schriftelijk en gemotiveerd binnen vier weken na ontvangst van het bezwaar. Indien het bezwaar als bedoeld in het vorige lid gegrond wordt verklaard, worden de door middel van de controlemaatregelen verkregen gegevens terstond vernietigd.
- Tevens worden maatregelen ingetrokken indien deze ten onrechte zijn genomen;

2.11 Procedure bij verzoek tot toegang medewerkersaccount

2.11.1 Toelichting

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 Curio 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.

2.11.2 Uitgangspunten

- Degene die toegang krijgt tot de gegevens 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 Curio 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.
- 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.

2.12 Clear Desk & Screen

2.12.1 Toelichting

We hanteren een clear desk beleid voor papieren documenten en verwijderbare opslagmedia en een clear screen beleid voor ICT-voorzieningen met een beeldscherm.
Het is niet nodig om alles wat op het bureau ligt op te ruimen (clean desk) maar het is wel verplicht om gevoelige informatie ontoegankelijk te maken voor onbevoegden (clear desk). Elk gevoelig gegeven mag niet onbewaakt worden achtergelaten op het bureau, of zichtbaar zijn op het scherm voor onbevoegden.
Elke medewerker speelt een belangrijke rol in het vermijden van ongeoorloofde toegang tot gevoelige informatie. Dit geldt zowel voor de toegang tot de informatiesystemen en toepassingen als voor de fysieke toegang tot lokalen, kantoorruimtes of tot documenten. De medewerking van alle medewerkers is van essentieel belang.

N.b.: wanneer alle lokalen, bureaus en werkruimtes zijn opgeruimd en er nergens papieren rondslingeren, betekent dit een groter comfortgevoel bij de medewerkers en een positieve indruk van de organisatie bij de bezoekers.

2.12.2 Randvoorwaarden

- Archiefruimtes en dossierkasten bevatten sloten, zodat ze fysiek afgesloten kunnen worden;
- Ruimtes met ICT middelen bevatten sloten;
- Er is bij iedere printer een afgesloten papierbak aanwezig;
- Er is op iedere schoollocatie een papierversnipperaar aanwezig;
- Onbevoegd gebruik van fotokopieerapparaten en andere reproductieapparatuur (bijvoorbeeld scanners) is niet mogelijk;
- Balieschermen zijn uit zicht van bezoekers geplaatst.

2.12.3 Uitgangspunten clear screen

- Computerschermen worden door medewerkers vergrendeld bij het verlaten van de werkplek, op Windows middels Windowstoets+L, op touch devices door kort op de aan-uit knop te drukken;
- Computerschermen vergrendelen automatisch na een vastgestelde periode.

2.12.4 Uitgangspunten clear desk

Alle medewerkers zorgen voor een opgeruimde klaslokaal/werkplek. Let hierbij ook op dat er geen (vertrouwelijke) informatie op prikborden, whiteboards, flipovers, notitieblokken en dergelijke staat geschreven.

Algemeen

- Alle medewerkers werken zoveel mogelijk digitaal en houden hun werkomgeving opgeruimd;
- Plan regelmatig een moment in om spullen op te ruimen;
- Lees e-mails digitaal, druk ze niet af;
- Handel papierwerk direct af;
- Schakel je PC na werktijd uit;
- ICT-middelen laat je ~~bij voorkeur~~ niet onbeheerd in de auto achter~~. Kan het echt niet anders, plaats de ICT-middelen uit het zicht en schakel ze volledig uit. Criminelen kunnen de apparaten namelijk middels sensoren opsporen, ook als ze in stand-by of vliegtuigmodus staan;~~
- Medewerkers spreken elkaar aan op ongewenst gedrag omtrent Clear desk & screen.

Documenten

- Los papierwerk is niet toegestaan, tenzij het niet anders kan. Als je twijfelt of je een papieren document nog nodig hebt, is het antwoord “nee”;
- Gevoelige informatie wordt altijd afgesloten opgeborgen aan het einde van de werkdag;
- Alle medewerkers vernietigen vertrouwelijke fysieke documenten indien ze deze niet meer nodig hebben. Ze worden weggegooid in de daarvoor bestemde afgesloten afvalbak en eerst versnipperd;
- Voorzie gevoelige informatie altijd van een map met daarop een stempel / sticker met de tekst ‘Vertrouwelijk’. Indien er geen stempel / sticker voorhanden is, schrijf dan op de map ‘Vertrouwelijk’.

Kopiëren en printen

- Informatie wordt uitsluitend geprint of gekopieerd indien noodzakelijk;
- Prints worden zoveel mogelijk beveiligd met een toegangscode (via de follow-me printers printers);
- Prints die direct worden afgedrukt (zonder toegangscode), worden meteen bij de printer opgehaald;

2.13 Consequenties van overtreding

2.13.1 Toelichting

Bij handelen in strijd met dit Reglement of algemeen geldende (wettelijke) regels, kan Curio 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.

2.13.2 Uitgangspunten

- 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 medewerker gelegenheid heeft gekregen zijn zienswijze naar voren te brengen.
- In afwijking van het voorgaande is het mogelijk dat Curio 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.

2.14 Melden datalek

Een datalek is onbedoelde of ongeoorloofde toegang tot persoonsgegevens, maar ook het ongewenst vernietigen, verliezen, wijzigen of verstrekken van persoonsgegevens. In de wet spreekt men van een inbreuk op de privacy.
Waar moet je aan denken?

- Een papieren document, gegevensdrager met persoonsgegevens verloren/gestolen.
  Bijvoorbeeld: een printje dat je hebt laten liggen, een tas in de trein laten staan, een USB stick verloren, laptop gestolen.
- Je ziet teveel gegevens in een applicatiescherm.
  Bijvoorbeeld: je hebt teveel rechten in een applicatie
- Je account is gehackt of je hebt inloggegevens gelekt.
  Bijvoorbeeld: Ransomware of je bent in een Phishing e-mail getrapt.
- Je hebt gegevens met de verkeerde persoon gedeeld of onjuist afgeleverd.
- Bijvoorbeeld: onjuiste adressering op een brief, e-mail naar verkeerd persoon gestuurd, verkeerde gegevens gedeeld in een telefoongesprek.

Zoals je in de voorbeelden kunt zien, gaat het dus om gegevens die je digitaal verwerkt, op “papier” staan of je mondeling (telefonisch) deelt.
Je bent als medewerker wettelijk verplicht een datalek te melden.