



DALTON STEDELIJK
LYCEUM
DORDRECHT

**Gedragcode verantwoord gebruik
bedrijfsmiddelen**

Inhoud

Gedragscode verantwoord gebruik bedrijfsmiddelen	1
1. Inleiding	5
1.1 Uitgangspunten gedragscode	5
1.2 Eigen verantwoordelijkheid en privégebruik.....	6
1.3 Verschillende soorten gegevens	6
2. Gedragscode.....	8
2.1 Algemene normen	8
2.2 Computergebruik.....	8
2.3 Werkplek.....	9
2.4 Gebruik eigen devices (Own Device)	9
2.5 Voorwaarden voor gebruik van een eigen device	9
2.6 Software en digitaal lesmateriaal	10
2.7 Gebruik van e-mail.....	10
2.8 Gebruik van internet.....	11
2.9 Verantwoord online.....	11
2.10 Sociale media	12
2.11 Gebruik beeld- en geluidsmateriaal.....	13
2.12 Wachtwoorden en pincodes.....	13
2.13 Meldplicht Datalekken.....	13
3. Controle gebruik bedrijfs-middelen	14
3.1 Voorwaarden voor controle	14
3.2 Uitvoering van de controle	14
3.3 Disciplinaire maatregelen	15
3.4 Bezwaar en beroep	15
3.5 Slotbepaling	15

1. Inleiding

Het gebruik van internet, computernetwerk, en e-mail is voor alle medewerkers van de school noodzakelijk om de werkzaamheden te kunnen verrichten. Bij deze werkzaamheden wordt gebruik gemaakt van veel gegevens, waaronder persoonsgegevens. De (ict)faciliteiten en de verschillende gegevens worden in dit document **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 365, administratiesystemen en (online)digitaal lesmateriaal maar ook apps op (mobiele) devices.*
- Informatie en (persoons)gegevens: *rapporages, leerling dossiers, 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 en maar ook sociale media zoals Facebook, LinkedIn, Instagram en Twitter.*

Aan het gebruik van deze bedrijfsmiddelen zijn risico's verbonden, waardoor het noodzakelijk is om hierover afspraken te maken. Van medewerkers van het Stedelijk Dalton Lyceum wordt verwacht dat zij veilig en verantwoord omgaan met de beschikbaar gestelde bedrijfsmiddelen. Dit wordt ook verwacht als medewerkers hun eigen middelen inzetten om werkzaamheden voor de school uit te voeren.

De afspraken in dit document gelden voor alle locaties van waaruit (school)werkzaamheden worden verricht en voor alle devices waarmee het werk wordt uitgevoerd. Ze gelden voor iedereen die werkzaam is bij het Stedelijk Dalton Lyceum, ook voor uitzendkrachten en tijdelijke werknemers.

1.1 Uitgangspunten gedragscode

Deze gedragscode legt regels vast voor het gebruik van de bedrijfsmiddelen door medewerkers en over de controle op de naleving hiervan.

Het doel van deze gedragscode is het vastleggen van normen en uitgangspunten ten aanzien van:

- systeem- en netwerkbeveiliging, inclusief beveiliging tegen schade en misbruik
- het tegengaan van seksuele intimidatie, discriminatie en andere strafbare feiten
- de 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
- de bescherming van vertrouwelijke informatie van het schoolbestuur, haar medewerkers, leerlingen en hun ouders
- het voorkomen en tegengaan van misbruik van de bedrijfsmiddelen
- de bescherming van de intellectuele eigendomsrechten van het schoolbestuur en derden
- het voorkomen van negatieve publiciteit
- kosten- en capaciteitsbeheersing

De controle op het gebruik van bedrijfsmiddelen is een verwerking van persoonsgegevens in de zin van de privacywetgeving. Het Stedelijk Dalton Lyceum 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.

1.2 Eigen verantwoordelijkheid en privégebruik

Het gebruik van door het Stedelijk Dalton Lyceum 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.

1.3 Verschillende soorten gegevens

Het Stedelijk Dalton Lyceum is verantwoordelijk voor het regelen van informatiebeveiliging en privacy. Het belangrijkste doel van informatiebeveiliging en privacy is het beschermen van gegevens.

Het Stedelijk Dalton Lyceum 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 het Stedelijk Dalton Lyceum bedoeld zijn. Denk na voordat je deze gegevens deelt met externen.
- **Vertrouwelijke gegevens;** dit zijn gegevens die alleen voor specifieke, hiervoor geautoriseerde medewerkers binnen het Stedelijk Dalton Lyceum 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 iedereen om zorgvuldig om te gaan met persoonsgegevens. Onderdeel van deze wettelijke verplichting is dat het Stedelijk Dalton Lyceum met leveranciers van (online) applicaties, waarin persoonsgegevens worden verwerkt, een verwerkersovereenkomst afsluit. Hierbij gaat het bijvoorbeeld om het verwerken van inloggegevens, wachtwoorden en het opslaan van door gebruikers gemaakt werk.

Het Stedelijk Dalton Lyceum heeft twee stafleden Onderwijs & ICT in dienst, waarvan één de deeltaak van privacy officer vervuld. Dit staflid communiceert intern de gedragsregels die horen bij het verwerken van persoonsgegevens. Deze dienen met uiterste zorgvuldigheid verwerkt en gedeeld te worden.

Als persoonsgegevens toegankelijk en of inzichtelijk zijn voor personen, die geen toegang behoren hebben tot deze gegevens is er sprake van een beveiligingsincident, waaruit mogelijk Kim van Schie, Gedragscode verantwoord gebruik bedrijfsmiddelen, 12-12-2025

een datalek kan voortkomen. Een dergelijk incident kan schadelijke gevolgen hebben voor de betrokkene(n) en het Stedelijk Dalton Lyceum.

Om op een veilige, verantwoorde en werkbare manier met deze gegevens om te gaan maakt het Stedelijk Dalton Lyceum 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 het Stedelijk Dalton Lyceum goedgekeurde bedrijfsmiddelen.

Van medewerkers van het Stedelijk Dalton Lyceum en/of externe medewerkers, die uit hoofde van hun functie toegang hebben tot de digitale informatiesystemen en hiermee tot bv. personeelsdossiers, vertrouwelijke enquêtegegevens, zorgdossiers et cetera wordt verwacht dat zij zorgvuldig omgaan met de functioneel aan hen beschikbaar gestelde informatie. 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.

2. Gedragscode

In deze gedragscode voor verantwoord gebruik van bedrijfsmiddelen geeft het Stedelijk Dalton Lyceum 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.

2.1 Algemene normen

Iedere medewerker voldoet minimaal aan de volgende algemene normen voor 'zorgvuldigheid':

- 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 aan privacy@dalton-dordrecht.nl of een telefonische melding bij de leidinggevende. (Hiervoor wordt verwezen naar de procedure meldplicht datalekken van het Stedelijk Dalton Lyceum).

2.2 Computergebruik

Voor het uitoefenen van de werkzaamheden stelt het Stedelijk Dalton Lyceum aan de medewerker computer- en netwerkfaciliteiten (ict-bedrijfsmiddelen) ter beschikking. Het gebruik van deze ict- bedrijfsmiddelen is verbonden aan deze werkzaamheden en gaat uit van 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 het Stedelijk Dalton Lyceum indien deze gegevens, om welke reden dan ook, elders opgeslagen worden.
- Deel wachtwoorden nooit, ook niet incidenteel. Wachtwoorden zijn persoonlijk.
- Sluit na gebruik de computer af of log uit.
- Meld storingen van beheerde werkplekken (computer of laptop) online bij de ict-afdeling via <https://topdesk.kienict.nl/> of via een e-mail aan helpdesk@kienict.nl.
- De medewerker is ervan op de hoogte dat vanuit KIEN-ict, in overleg, de computer kan worden overgenomen om gesignaleerde problemen op te lossen.

Sinds augustus 2021 beschikt iedere medewerker van het Stedelijk Dalton Lyceum over een door de school beheerd device in bruikleen, tenzij de medewerker een vaste werkplek heeft met een vaste pc. Deze vaste werkplekken vormen een uitzondering en beschikken over een door de school beheerde computer die voldoet aan de juiste beveiligingseisen. Alle beheerde devices worden onderhouden door KIEN ICT en voldoen aan de actuele

beveiligingsstandaarden. Medewerkers wordt daarom sterk aangeraden om schoolwerkzaamheden uitsluitend op deze beheerde devices uit te voeren.

2.3 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-mail programma af en zorg voor een opgeruimd digitaal bureaublad.
- Laat geen afdrucken 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 meldplicht datalekken van het Stedelijk Dalton Lyceum. Deze procedure is terug te vinden op het Intranet (zal na instemming van MR worden geplaatst)

2.4 Gebruik eigen devices (Own Device)

Niet alle medewerkers beschikken over een eigen laptop. Medewerkers die een vaste werkplek met een vaste pc hebben, hebben doorgaans geen eigen device nodig om schoolwerkzaamheden te verrichten.

Wanneer een medewerker wél over een eigen device beschikt, wordt het gebruik daarvan voor schoolwerkzaamheden niet aanbevolen, omdat deze apparaten meestal niet dezelfde beveiligingsniveaus bereiken als beheerde devices en dit geldt ook voor het beveiligingsniveau van het netwerk (KIENroam t.o.v. Eduroam).

In incidentele situaties kan het gebruik van een eigen device worden gedoogd, mits wordt voldaan aan onderstaande voorwaarden.

Let op: Het gebruik van een eigen device is alleen toegestaan wanneer de medewerker op dat moment geen toegang heeft tot een bruikleen-device of vaste schoolcomputer die door KIEN ICT wordt beheerd.

2.5 Voorwaarden voor gebruik van een eigen device

Wanneer een medewerker ervoor kiest of genooddaakt is schoolwerkzaamheden op een eigen device uit te voeren, rust de verantwoordelijkheid voor passende beveiligingsmaatregelen volledig bij de medewerker. De volgende voorwaarden gelden minimaal:

- Het device is beveiligd met een sterk wachtwoord (14 karakters, bevat minimaal hoofdletters, kleine letters, cijfers en speciale tekens), of – bij smartphone/tablet – een pincode van minimaal 4 tekens (bij voorkeur langer).

- Vergrendel het device direct bij het verlaten van de werkplek (bijv. via *Windows-toets + L*).
- Sla nooit persoonsgegevens van het Stedelijk Dalton Lyceum op een eigen device op. Dit is niet toegestaan.
- Alle overige gegevens die betrekking hebben op het Stedelijk Dalton Lyceum mogen uitsluitend versleuteld worden opgeslagen en mogen niet op het schoolnetwerk worden geplaatst.
- Houd privégegevens en (versleutelde) schoolgegevens strikt gescheiden en zorg dat deze scheiding duidelijk herkenbaar is.
- Zorg dat het device maandelijks wordt bijgewerkt met beveiligings- en systeemupdates.
- Bescherm het device tegen virussen en malware met een actuele virusscanner en voer minimaal maandelijks een volledige scan uit.
- Vergeet de downloadmap niet: verwijder na gebruik direct bijlagen en/of andere gedownloade documenten van het Stedelijk Dalton Lyceum.

Het Stedelijk Dalton Lyceum mag controles uitvoeren op bovenstaande maatregelen. Op verzoek van Het Stedelijk Dalton Lyceum moet de medewerker zelf aantonen dat de bovenstaande maatregelen worden toegepast.

2.6 Software en digitaal lesmateriaal

Het gebruik van digitaal lesmateriaal is niet weg te denken bij het Stedelijk Dalton Lyceum. 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 van betrokkenen, 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 het Stedelijk Dalton Lyceum alleen toegestaan met de juiste licenties en na het nemen van eventuele aanvullende (beveiligings)maatregelen.
- Bij het gebruik van online software, app's en digitaal lesmateriaal, wordt vooraf gekeken of er persoonsgegevens bij verwerkt worden.
- Een verwerkersovereenkomst wordt afgesloten met elke leverancier van (online)software, die in opdracht van het Stedelijk Dalton Lyceum persoonsgegevens verwerkt. Dit wordt voorafgaand aan het gebruik geregeld.
- Aanvragen van digitaal lesmateriaal en/of andere software volgt bij het Stedelijk Dalton Lyceum de afgesproken aanvraagprocedure. Hiervoor is een aanvraagformulier beschikbaar dat als uitgangspunt dient voor eventuele wettelijk verplichte aanvullende privacy- en/of beveiligingsmaatregelen. Procedure en aanvraagformulier zijn beschikbaar via het intranet van het SDL: [2025 Stappenplan aanschaf nieuwe software \(4\).pdf](#)

2.7 Gebruik van e-mail

Het Stedelijk Dalton Lyceum stelt een e-mailsysteem en een bijbehorende mailbox aan de medewerker ter beschikking voor het uitoefenen van de werkzaamheden. Gebruik van e-mailfaciliteiten is verbonden aan deze werkzaamheden en gaan uit van de volgende afspraken:

- Gebruik het school e-mail adres alléén voor school gerelateerde zaken.
- Gebruik voor privé e-mail een eigen privé e-mailadres via een externe webmaildienst. (gebruik bijvoorbeeld via een browser de 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.
- Het is niet toegestaan e-mail te gebruiken voor:
 - het verzenden van berichten met pornografische, racistische, discriminerende, beledigende, (seksueel) intimiderende of aanstootgevende inhoud
 - het verzenden van berichten die kunnen aanzetten tot haat en geweld.
 - het verzenden van berichten die het Stedelijk Dalton Lyceum in diskrediet brengen of anderszins beschadigen
 - het verzenden van BSN-nummers en/of gezondheidsgegevens van medewerkers en/of leerlingen
- Het (automatisch) doorsturen van e-mail naar een privé email-adres is niet toegestaan. Elke medewerker heeft een office 365 account, waarmee eenvoudig online de mail kan worden gelezen.
- Synchroniseert een medewerker de school toch e-mail met een eigen devices (tablet, telefoon) dan kan het Stedelijk Dalton Lyceum, 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.
- Herkennen en omgaan met malware waaronder phishing en ransomware die via e-mail binnenkomt wordt als bekend geacht.
- Een mailbox is geen opslagplaats voor data. Sla belangrijke bijlagen en/of e-mail berichten zodanig op, dat ze eenvoudig terug te vinden zijn.

2.8 Gebruik van internet

Het Stedelijk Dalton Lyceum stelt het gebruik van internet en de bijbehorende faciliteiten aan de medewerker ter beschikking voor het uitoefenen van de werkzaamheden. 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 niet toegestaan om
 - op internet sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten
 - films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van een evident illegale bron
 - onder leestijd 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.

2.9 Verantwoord 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.

Het Stedelijk Dalton Lyceum 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 waaronder phishing en ransomware is, het kunnen herkennen en weten hoe te handelen;
- Terughoudend zijn met het online achterlaten van gegevens met betrekking tot het Stedelijk Dalton Lyceum;
- 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 eduroam of het eigen draadloze netwerk thuis is)

2.10 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 het Stedelijk Dalton Lyceum ook als zij online een privémening verkondigen.

Bij het Stedelijk Dalton Lyceum 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 het Stedelijk Dalton Lyceum en iedereen die hierbij betrokken is.
- Maak bij onderwijs gerelateerde onderwerpen duidelijk of publicatie op persoonlijke titel of namens het Stedelijk Dalton Lyceum gedaan wordt.
- Publiceer geen vertrouwelijke informatie op sociale media.
- Publiceer geen beeldmateriaal van leerlingen zonder de uitdrukkelijke voorafgaande vastgelegde 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 het Stedelijk Dalton Lyceum.
- Het is medewerkers niet toegestaan om met een privé account '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.
- Medewerkers gebruiken onderling Microsoft Teams voor de online communicatie. Het advies is om geen gebruik te maken van andere communicatiekanalen zoals Whatsapp of Signal.
- Het gebruik van WhatsApp in de communicatie met leerlingen is niet toegestaan. Gebeurt dit toch? Deel dan in ieder geval geen persoonsgegevens.

2.11 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 het Stedelijk Dalton Lyceum 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.

- Het Stedelijk Dalton Lyceum verwijst hierbij naar de richtlijn die is opgesteld voor het gebruik en toestemming van beeldmateriaal.
- 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.

2.12 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 **14** tekens bevatten.
- Pincodes (op telefoon of tablet) moeten langer zijn dan 4 tekens.
- Wijzigen van het wachtwoord voor het netwerk wordt bij het Stedelijk Dalton Lyceum drie keer per jaar afgedwongen. Van medewerkers wordt verwacht dat zij op die momenten ook het wachtwoord tot Magister en eventuele andere informatiesystemen wijzigen.
- Gebruik niet voor elke systeem hetzelfde wachtwoord.
- Deel wachtwoorden nooit, ook niet incidenteel. Wachtwoorden zijn persoonlijk.

2.13 Meldplicht Datalekken

Van alle medewerkers wordt verwacht dat zij beveiligingsincidenten en mogelijke datalekken melden via privacy@dalton-dordrecht.nl of direct doorgeven aan hun leidinggevende. Medewerkers worden geacht bekend te zijn met de procedure meldplicht datalekken van het Stedelijk Dalton Lyceum.

3. Controle gebruik bedrijfsmiddelen

Het Stedelijk Dalton Lyceum handelt bij de controle op het gebruik van bedrijfsmiddelen binnen de geldende wet- en regelgeving, te weten:

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

Het Stedelijk Dalton Lyceum 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.

3.1 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 voorzitter College van Bestuur 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 voorzitter College van Bestuur, 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. Het Stedelijk Dalton Lyceum 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.

3.2 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 het Stedelijk Dalton Lyceum worden de nodige maatregelen getroffen, opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn.
- Door het Stedelijk Dalton Lyceum worden passende technische en organisatorische maatregelen getroffen om persoonsgegevens te beveiligen tegen verlies en/of tegen enige vorm van onrechtmatige verwerking.

3.3 Disciplinaire maatregelen

Bij het handelen in strijd met deze gedragscode of de algemeen geldende wettelijke regels, kan het bestuur van het Stedelijk Dalton Lyceum, 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.

3.4 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. Hiervoor gelden de regels vanuit de arbeidsovereenkomst, regels rondom personeelszaken en/of de van toepassing zijnde CAO.

Dit document heeft betrekking op verwerking van persoonsgegevens en/of controle van het gedrag of de prestaties van medewerkers. Het medezeggenschapsorgaan (de MR) is om deze reden instemmingsplichtig.

De organisatie kan deze gedragscode met instemming van de MR wijzigen als de omstandigheden daar aanleiding toe geven. Voorgenomen wijzigingen worden voorafgaand aan de invoering ervan aan de medewerkers bekend gemaakt.

3.5 Slotbepaling

Deze regeling wordt jaarlijks geëvalueerd door het Stedelijk Dalton Lyceum en de MR.