Gedragscode ICT en sociale media leerlingen & medewerkers LdV

(IBP: informatiebeveiliging & privacy)

1 februari 2022

1. Inleiding & doel

Het gebruik van internet, het computernetwerk en e-mail is voor alle leerlingen en medewerkers van Scholengroep Leonardo da Vinci noodzakelijk om schoolwerkzaamheden te verrichten. Voor het uitoefenen van schoolwerkzaamheden worden computer- en netwerkfaciliteiten (bedrijfsmiddelen) beschikbaar gesteld. Daarnaast maken we gebruik van veel informatie, waaronder persoonsgegevens. Aan het gebruik van bedrijfsmiddelen en het gebruik van informatie zijn risico's verbonden die het stellen van gedragsregels noodzakelijk maken. Wij moeten ons daarnaast houden aan wet- en regelgeving.

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

a. bescherming van privacygevoelige en vertrouwelijke informatie waaronder persoonsgegevens;
b. systeem- en netwerkbeveiliging, inclusief beveiliging tegen schade en misbruik;
c. tegengaan van seksuele intimidatie, discriminatie en andere strafbare feiten;
d. het voorkomen en tegengaan van misbruik van de bedrijfsmiddelen;
e. bescherming van de intellectuele eigendomsrechten waaronder het respecteren van de licentie-afspraken die van toepassing zijn binnen de scholengroep;
f. voorkomen van negatieve publiciteit;
g. kosten- en capaciteitsbeheersing.

1.1 Reikwijdte en begripsbepalingen

1. Deze gedragscode geldt voor:
   a. alle locaties en werkplekken binnen de scholengroep van waaruit (school)werkzaamheden worden verricht;
   b. alle devices waarmee (school)werkzaamheden worden uitgevoerd.
2. Begripsbepalingen:
   a. Bedrijfsmiddelen: 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 Office, administratiesystemen en (online)digitaal lesmateriaal maar ook apps op (mobiele) devices;
      - *Informatie en (persoons)gegevens*: rapportages, 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, diensten om bestanden over te dragen zoals Facebook, LinkedIn, Instagram en Twitter.

   b. gebruikers:
      - alle leerlingen;
      - alle medewerkers: iedereen die werkzaam is bij de scholengroep (ook uitzendkrachten, tijdelijke werknemers, stagiaires, studenten etc.).

      (In dit document worden beide doelgroepen met 'je' aangesproken omdat alle uitgangspunten in dit document in beginsel gelden voor beide doelgroepen (tenzij anders wordt vermeld), om de gelijkheid en de dialoog te bevorderen en het gezamenlijke bewustzijn te vergroten.)
   c. scholengroep: Stichting Scholengroep Leonardo da Vinci Leiden.

1.2 Informatievoorziening

Deze gedragscode is van toepassing op alle leerlingen en medewerkers en wordt aan gebruikers ter beschikking gesteld en onder de aandacht gebracht.

1.3 Het delen van (persoons)gegevens

1. De scholengroep onderscheidt drie typen gegevens:
   a. openbare gegevens: dit zijn gegevens die juist voor publicatie zijn bedoeld;
   b. interne gegevens; dit zijn gegevens die alleen voor intern gebruik en verwerking zijn bedoeld;
   c. vertrouwelijke gegevens; dit zijn gegevens die alleen voor specifieke, hiervoor geautoriseerde medewerkers toegankelijk zijn.
2. Van de gebruiker wordt verwacht dat hij/zij zorgvuldig omgaat met de beschikbaar gestelde informatie, dat de privacywetgeving wordt nageleefd en dat op geen enkele wijze informatie, waarvan redelijkerwijze kan worden aangenomen dat deze vertrouwelijk of privacygevoelig is, zonder toestemming van betrokkene of leidinggevende wordt gebruikt en/of naar buiten wordt gebracht.

2. Afspraken

2.1 Gebruik schoolnetwerk

Het gebruik van het schoolnetwerk wordt aan de gebruiker voor het uitoefenen van de schoolwerkzaamheden beschikbaar gesteld. Hiervoor geldt het volgende:

a. gebruik van het schoolnetwerk mag de kwaliteit van het (draadloze) netwerk niet in gevaar brengen of schade aan personen of instellingen veroorzaken;
b. het schoolnetwerk is alleen toegankelijk voor geregistreerde gebruikers;
c. gebruikers mogen alleen met het eigen account gebruik maken van het netwerk;
d. na gebruik sluit de gebruiker het eigen account af;
e. de gebruiker neemt bij (vermoeden van) misbruik van zijn/haar gegevens of bij (vermoeden van) inbreuken op de beveiliging van het schoolnetwerk, van binnenuit of van buiten de school, direct contact op met de privacy officer van de school;
f. het is verboden om zich moedwillig toegang te verschaffen tot andermans gegevens of bestanden;
g. onbedoelde inbreuk op beveiliging, van binnenuit of van buiten de school dient onmiddellijk aan de schoolleiding gemeld te worden.

2.2 Gebruik bedrijfsmiddelen

Het gebruik van bedrijfsmiddelen wordt aan de gebruiker voor het uitoefenen van de schoolwerkzaamheden beschikbaar gesteld. Hiervoor geldt het volgende:

a. gebruik een device dat beveiligd is met een wachtwoord en een veilige netwerkverbinding (bijvoorbeeld via VPN of een met wachtwoord beveiligde wifi);
b. voorkom dat anderen (onbedoeld) toegang kunnen krijgen tot bedrijfsmiddelen waartoe zij geen rechten hebben en laat gegevens niet (onbedoeld) lekken;
c. zorg dat privacygevoelige gegevens niet toegankelijk zijn voor onbevoegden;
d. 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;
e. sla (persoons)gegevens alleen op de daarvoor aangewezen systemen op (opslaan van gegevens in public Cloud omgevingen, zoals een persoonlijke dropbox, is niet toegestaan);
f. het downloaden en installeren van software uit de Windows Store op de computer van de scholengroep is toegestaan;
g. sla alleen gegevens op in de hiervoor opgezette omgeving/ teams in office 365 en niet op het devices zelf zoals op de harde schijf;
h. stel vragen of meld storingen bij de ICT-afdeling via servicedesk@ldvleiden.nl

2.3 Gebruik eigen devices

De scholengroep is verantwoordelijk voor het implementeren van de juiste beveiligingsmaatregelen als het gaat om de bedrijfsmiddelen van de school. Als gebruiker een eigen device voor schoolwerkzaamheden gebruikt, dan wordt verwacht dat gebruiker minimaal de volgende beveiligingsmaatregelen neemt:

a. bescherm de toegang met een wachtwoord of, in het geval van een iPad of tablet, met een pincode;

b. wanneer het apparaat (weer) in gebruik wordt genomen, moet het om een wachtwoord of pincode vragen;
c. het is niet toegestaan om persoonsgegevens van de scholengroep op het eigen device op te slaan;
d. versleutel gegevens als deze toch, om welke reden dan ook, niet op het schoolnetwerk opgeslagen (kunnen) worden;
e. scheid versleutelde gegevens en privégegevens van elkaar: deze scheiding moet duidelijk herkenbaar zijn op het eigen device;
f. houd periodieke software updates (minimaal maandelijks);
g. neem goede maatregelen tegen virussen of malware.

2.4 Eigen verantwoordelijkheid

1. Gebruiker tekent een bruikleenovereenkomt voor de bedrijfsmiddelen die aan hem/haar in bruikleen zijn gegeven. Gebruiker is verantwoordelijk voor een in bruikleen gegeven bedrijfsmiddel en bewaart deze altijd op een veilige plek, ook tijdens de schoolvakanties.
2. Iedere gebruiker voldoet aan de algemene normen voor 'zorgvuldigheid'. Dit zijn (onder andere):
   a. zorgvuldig omgaan met persoonsgegevens;
   b. zorgdragen voor goede fysieke en technische bescherming van de bedrijfsmiddelen;
   c. zorgdragen voor goede technische bescherming van de bedrijfsmiddelen;
   d. voorkomen van het lekken van interne en vertrouwelijke informatie;
   e. voorkomen dat beveiligingsmaatregelen worden omzeild;
   f. onmiddellijk na constatering melden van verloren of gestolen bedrijfsmiddelen door contact op te nemen met de Privacy Officer van de eigen school.

2.5 Werkplek

1. Gebruiker werkt in een omgeving waar anderen niet kunnen meekijken en/of luisteren en gebruikt indien nodig een headset of koptelefoon.
2. Voor de werkplek gelden de volgende regels:
   a. vergrendel bij het tijdelijk verlaten van de werkplek de pc (windowstoets+L) en sluit na gebruik de computer af of log uit:
   b. verwijder vertrouwelijke documenten van het bureau bij het voor langere tijd verlaten van de werkplek;
   c. voorkom dat 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;
   d. laat geen afdrukken bij de printer liggen, zeker niet als er persoonsgegevens op staan;
   e. haal overbodig geworden papieren documenten met persoonsgegevens altijd door de papierversnipperaar of deponeer ze in speciaal hiervoor bestemde vertrouwelijke papiercontainers.

2.6 E-mail

Voor het gebruik van de door de scholengroep beschikbaar gestelde e-mailfaciliteiten geldt het volgende:

a. gebruik het school e-mail adres alléén voor school gerelateerde zaken;
b. gebruik voor privé e-mail een eigen privé e-mailadres;
c. het ontvangen/versturen van privémail op het school e-mailadres is niet toegestaan;
d. het versturen van e-mail moet voldoen aan de normale gedragsregels die gelden voor schriftelijke correspondentie en mag niet gebruikt worden voor 'verboden handelingen' (zie ook 2.12);
e. indien de school e-mail met een eigen devices wordt gesynchroniseerd, dan kan de scholengroep, bij verlies of diefstal van het device, gebruik maken van de mogelijkheid om de e-mail op afstand te wissen, ook als daarmee (privé)gegevens van het device gewist worden.
f. persoonsgegevens worden niet per e-mail verzonden (en worden niet op een USB-stick geplaatst). Voor het (in- en extern) delen van werk gerelateerde (versleutelde) persoonsgegevens gelden speciale afspraken. Deze komen te staan in de medewerkersTeams van de eigen school.

2.7 Bewust veilig online

1. Internet en de bijbehorende faciliteiten worden aan de gebruiker onder andere voor het uitoefenen van schoolwerkzaamheden, zowel tijdens en buiten de lestijden, beschikbaar gesteld.
2. De scholengroep verwacht van gebruikers dat zij:
   a. het onderscheid kennen tussen veilige en onveilige netwerken en websites;
   b. bij het verwerken van persoonsgegevens alléén gebruik maken van bekende én beveiligde draadloze netwerken;
   c. weten wat malware is, het kunnen herkennen en weten hoe te handelen;
   d. terughoudend zijn met het online achterlaten van gegevens met betrekking tot de scholengroep;
   e. controleren of er daadwerkelijk van een bekend én beveiligd netwerk gebruik gemaakt wordt bij het bezoek aan openbare ruimtes.
3. Het is niet toegestaan:
   a. op internet sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend, gewelddadig, aanstootgevend of anderszins onacceptabel materiaal bevatten;
   b. te hacken, overmatig downloaden of overbelasten van het netwerk;
   c. iemand lastig te vallen, te beledigen of achtervolgen;
   d. ongeoorloofd toegang te krijgen tot niet-openbare sites of programma's;
   e. informatie, foto's of video's te delen waarvan duidelijk is dat die niet bedoeld zijn om verder te verspreiden;
   f. films, muziek, software en auteursrechtelijk beschermd materiaal te downloaden van een evident illegale bron;
   g. tijdens de lestijd spelletjes te spelen en gamewebsites te bezoeken, anders dan in opdracht van en met toestemming van de docent;
   h. tijdens de lestijd chatboxen of vergelijkbare toepassingen te bezoeken, anders dan in het kader van lesopdrachten;
   i. deel te nemen aan kansspelen;
   j. 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 gebruikers. Dit geldt ook voor internetgebruik buiten het schoolnetwerk met betrekking tot aan de school verbonden gebruikers/personen.
4. Wanneer gebruiker per ongeluk een ongewenste site opent of software installeert, meldt gebruiker dit aan de leraar/leidinggevende.

2.8 Gebruik beeld- en geluidsmateriaal

1. Voor het gebruiken, maken en delen van beeld- en geluidsmateriaal, het delen van foto's en video's gelden de volgende regels:
   a. Het is niet toegestaan om film, video-, en/of geluidsopnamen of ander materiaal van leerling en medewerker of andere bij de school betrokken personen te maken en/of via (elektronische) informatie- en communicatiemiddelen openbaar te maken, tenzij hiervoor expliciet en aantoonbaar toestemming is gegeven.
   b. Indien betrokkene een leerling is moet vooraf toestemming worden gegeven door ouders als de leerling jonger is dan 16 jaar of de leerling zelf als deze ouder dan 16 jaar is.
2. Voor de (overige) privacyregels met betrekking tot beeld- en geluidsmateriaal verwijzen wij naar het protocol foto-en filmopnamen en cameratoezicht van de scholengroep.

2.9 Wachtwoorden en pincodes

1. Wachtwoord, inlognaam en pincode zijn persoonlijk, deze worden niet genoteerd en worden niet gedeeld, ook niet incidenteel.
2. Gebruiker laat de internetbrowser nooit een wachtwoord onthouden.
3. Gebruiker zorgt ervoor dat de beamer/smartbord uit of op "freeze" staat wanneer het wachtwoord wordt ingetypt.
4. De (overige) regels over het veilig gebruik van wachtwoorden en pincodes staan in het Autorisatie- en toegangsbeleid van de scholengroep.

2.10 Software en digitaal lesmateriaal (medewerkers)

1. Voor het gebruik van nieuw digitaal lesmateriaal kun je een aanvraag doen bij de afdeling ICT. Het uitgangspunt hierbij is dat wordt voldaan aan wettelijk verplichte aanvullende privacy- en/of beveiligingsmaatregelen.
2. Bij het gebruik van online software, apps en digitaal lesmateriaal, wordt gekeken of er persoonsgegevens verwerkt worden.
3. Het installeren van software wordt alleen toegestaan met de juiste licenties, na het nemen van eventuele aanvullende maatregelen en indien er persoonsgegevens worden verwerkt na het afsluiten van een verwerkersovereenkomst met de leverancier van (online)software.

2.11 Systemen (bv. leerlingvolgsysteem of personeelsinformatiesysteem) (medewerkers)

1. Wanneer gebruiker gegevens verwerkt, worden deze zorgvuldig geformuleerd, op een manier zodat de betrokkene deze tekst kan lezen en begrijpen.
2. Opvragen van gegevens uit deze systemen doet gebruiker alleen op een bedrijfsmiddel van school of een bedrijfsmiddel dat voldoet aan de beveiligingseisen van school.

2.12 Verboden handelingen

Het is niet toegestaan om bij wet verboden handelingen uit te voeren op een bedrijfsmiddel dat voor schoolwerkzaamheden gebruikt wordt. Dit zijn (onder andere):

a. het opslaan of delen van illegale en/of aanstootgevende bestanden;
b. criminele activiteiten;
c. het gebruik van illegale software en/of het omzeilen van licenties;
d. uitvoeren van handelingen en/of installeren van software waardoor de veiligheid en stabiliteit van het netwerk en/of de vertrouwelijkheid van gegevens in gevaar komt.

2.13 Controle

In bijzondere situaties is het onderzoeken van systemen door het ICT team is toegestaan. De gegevens blijven privé en worden met de grootst mogelijke zorgvuldigheid behandeld. Controle en/of doorspelen van persoonlijke gegevens gebeurt slechts en alleen om zwaarwegende redenen.

3. Sociale media

Sociale media is een verzamelnaam voor alle internettoepassingen die het mogelijk maken om informatie met elkaar te delen. Het gaat hierbij om informatie in de vorm van tekst, geluid en/of beeld. De essentie van sociale media is dat iemand informatie deelt over zichzelf, over anderen of over een bepaald onderwerp.
Sociale media spelen een belangrijke rol in het onderwijs. Sociale media kunnen het onderwijs verbeteren maar brengen ook risico's met zich mee, zoals pesten en het ongewild delen van foto's of andere gegevens. Aan de hand van afspraken kan het gesprek op school, in de klas en ook thuis gevoerd worden over wat er acceptabel is op sociale media (en wat niet). Onderstaande afspraken en regels zijn van toepassing bij onze scholengroep en gelden onafhankelijk van de plaats waar we sociale media gebruiken: op school, in de klas en in het mediagebruik buiten de school.

Vooraf

1. Zorg dat je weet hoe de sociale media werken voordat je ze gebruikt, dat de instellingen goed staan en je niet meer informatie deelt dan je wilt /nodig is.
2. Realiseer je steeds dat publicaties op sociale media altijd vindbaar en moeilijk vernietigbaar zijn.
3. Houd rekening met de goede naam van (de scholen van) de scholengroep en iedereen die daarbij betrokken is.
4. Help elkaar om goed en verstandig met sociale media om te gaan en spreek elkaar hierop aan.
5. Je bent zelf/persoonlijke verantwoordelijk voor wat je plaatst op sociale media, ook het doorsturen (forwarden) en herplaatsen (retweeten) zijn handelingen waarop je kunt worden aangesproken.
6. Verstuur geen anonieme berichten, verzin geen berichten en gebruik geen fictieve of andere naam.
7. Zet geen vertrouwelijke informatie op sociale media.
8. Houd je wachtwoord geheim.
9. Communiceer via sociale media alleen voor acceptabele doeleinden en op een acceptabele manier (zie 2.7).

10. Maak bij onderwijs gerelateerde onderwerpen duidelijk of de publicatie op persoonlijke titel of namens de scholengroep wordt gedaan.
11. Neem contact op met een docent of leidinggevende als er twijfel bestaat over een publicatie of over de raakvlakken met de scholengroep.
12. Denk zorgvuldig na over het leggen van contact, het volgen van elkaar of 'vriend worden' of 'vriend blijven': maak een bewuste keuze en weet wie de andere persoon is.

Inhoud

13. Respecteer elkaars privacy.
14. Als je iets niet zou doen in real life, doe het dan ook niet online.
15. Behandel elkaar netjes en met respect en laat iedereen in zijn waarde.
16. Pest, kwets, stalk, bedreig en beschadig elkaar niet, maak elkaar niet zwart en sluit niemand buiten.
17. Publiceer geen informatie of beeldmateriaal van anderen zonder de uitdrukkelijke voorafgaande aantoonbare toestemming van betrokkene. Als betrokkene een leerling is, is toestemming nodig van ouders als de leerling jonger is dan 16 jaar of van de leerling zelf als deze ouder is dan 16 jaar.

Tijdens (live en online) lessen/schoolactiviteiten - leerlingen

18. Het gebruik van mobiele telefoon of sociale media is tijdens de les alleen toegestaan wanneer de leraar vooraf, in verband met het leerproces, toestemming geeft om hiervan gebruik te maken.
19. Tijdens examens, toetsen, overhoringen en proefwerken gelden aangepaste regels.
20. Tijdens schoolactiviteiten zoals excursies is het gebruik van internet en sociale media alleen toegestaan tijdens de heen- en terugreis.
21. Videolessen met leraren en leerlingen mogen niet worden opgenomen, bewerkt of gedeeld op social media of op een andere manier.
22. Je neemt alleen deel aan videolessen waarvoor je bent uitgenodigd.

Speciaal voor medewerkers

23. Bij onderwijsonderwerpen maken medewerkers duidelijk of zij op persoonlijke titel of namens de school publiceren.
24. Medewerkers zijn altijd vertegenwoordiger van de school – ook als zij een privémening verkondigen.
25. Bij twijfel over publiceren of over de raakvlakken met de school zoeken medewerkers contact met hun leidinggevende.
26. Ga niet in discussie met een leerling of ouder op social media.
27. Inzetten van sociale media in het lesprogramma is gebonden aan de toestemming van ouders als leerlingen jonger zijn dan 16 jaar.
28. Contact tussen medewerkers met leerlingen of met een groep leerlingen gaat via de software van de school. Het hiervoor gebruiken van sociale media (waaronder Whatsapp) is niet toegestaan. Dit contact kan plaatsvinden via het gebruik van (de klassenteams binnen) Teams.
29. Contact tussen medewerkers met ouders of met een groep ouders gaat via de software van de school. Het hiervoor gebruiken van sociale media (waaronder Whatsapp) is niet toegestaan. Dit contact kan plaatsvinden via de email-functie of de chatfunctie van Teams van het schoolaccount.
30. Wanneer een ouder belt of contact zoekt via social media checken we (bijvoorbeeld via controle vragen of terugbellen op het bij ons bekende nummer) of we ook inderdaad contact hebben met de ouder waar de contactzoeker zich voor uitgeeft.
31. Het plaatsen van facebook berichten met schoolinformatie en/of informatie over leerlingen is alleen toegestaan via de beheerder van de officiële facebookpagina van de school. De beheerder is zich ervan bewust dat de facebookberichten gedeeld worden.

4. Inwerkingtreding en slotbepaling

Deze gedragscode treedt in werking op 1 februari 2022, wordt om de vier jaar geëvalueerd en indien nodig tussentijds gewijzigd. Voorgenomen wijzigingen worden – ter instemming – voorgelegd aan de GMR en voorafgaand aan de invoering aan de medewerkers bekend gemaakt.