ICT-POLICY

gemeente Kasterlee basisonderwijs

mei 2019

INHOUD

Hoofdstuk 1 Draagwijdte en toepassingsgebied

Art.1 Deze ICT-policy is een reglement van inwendig bestuur en heeft een afdwingbaar karakter.

Art.2 Deze ICT-policy is ondergeschikt aan dwingende wetsbepalingen en hun uitvoeringsbesluiten.

Art.3 Deze policy regelt de toegang, het intern en extern gebruik en de controle van de ICT-infrastructuur die door de onderwijsinstelling en/of het schoolbestuur ter beschikking wordt gesteld van het personeelslid. Bedoeld worden onder andere de computer- en netwerkinfrastructuur (hardware en software), e-mail, internet, intranet, printers, kopieermachines, telefonie, gsm en fax evenals eventueel toekomstige elektronische media. Deze policy geldt eveneens voor alle gegevens die via deze systemen worden geproduceerd, overgedragen of erin worden opgeslagen.

Art.4 Deze ICT-policy is van toepassing op al het onderwijspersoneel van het gemeentebestuur van gemeente Kasterlee.

Hoofdstuk 2 Eigendom en verantwoordelijkheid

Art.5 De ICT-infrastructuur die aan het personeelslid ter beschikking is gesteld, blijft eigendom van het schoolbestuur.

Art.6 Het personeelslid draagt als een goede huisvader zorg voor de ICT-infrastructuur die hem ter beschikking is gesteld. Hij gebruikt deze middelen op een professioneel, sociaal, ethisch en juridisch correcte wijze, overeenkomstig de bepalingen in deze policy en de instructies die ter zake worden gegeven.

Art.7 Het personeelslid mag geen software die ter beschikking gesteld wordt door de onderwijsinstelling, transfereren naar eigen apparatuur, behoudens toestemming van het schoolbestuur of diens afgevaardigde.

Art.8 Elk personeelslid is verantwoordelijk voor zijn communicatiegedrag.

Art.9 Het schoolbestuur is niet verantwoordelijk voor misdrijven die door personeelsleden worden begaan.

Hoofdstuk 3 Toegang en bescherming

Art.10 Gebruikersnaam en wachtwoord

§1 De toegang tot de ICT-infrastructuur wordt verleend op basis van een gebruikersnaam en een wachtwoord.

§2 Het personeelslid mag uitsluitend met zijn eigen gebruikersnaam en wachtwoord inloggen. Het is niet toegestaan de gebruikersnaam en het wachtwoord van iemand anders te gebruiken, behalve met uitdrukkelijke toestemming van de eigenaar ervan of indien de continuïteit van de dienstverlening in het gedrang komt en niet op een andere manier kan worden gegarandeerd.

§3 Elk personeelslid is verantwoordelijk voor het bewaren van zijn gebruikersnaam en wachtwoord.

§4 Niemand mag zijn gebruikersnaam of wachtwoord aan onbevoegden doorgeven en/of door onbevoegden laten gebruiken.

§5 Zorg ervoor dat jouw paswoorden voldoende complex zijn en verander ze regelmatig:

- Minstens 9 karakters

- Hoofdletters en kleine letters
- minstens 1 cijfer
- minstens 1 speciaal karakter
- geen voor de hand liggende paswoorden

Art.11 Het personeelslid neemt de nodige veiligheidsmaatregelen om schade aan de ICT-infrastructuur te voorkomen, zowel binnen de onderwijsinstelling als daarbuiten (laptop, gsm,…). Draagbare ICT-infrastructuur (laptop, gsm,…) mag nooit onbewaakt op een openbare plaats of zichtbaar in een voertuig worden achtergelaten.
Volgende richtlijnen moeten in acht genomen worden:

- computers, laptops, externe gegevensdragers (harde schijven, USB-sticks,…) bevatten geen privacygevoelige info tenzij in een versleutelde, beveiligde map. Gegevens worden sowieso niet lokaal maar op de server / google-drive bewaard
- automatisch aanmelden voor laptops en andere programma's uitschakelen
- uitdrukkelijk opletten met toegangen tot persoonlijke accounts
- beter geen persoonlijke gegevens op hardware van de school plaatsen
- beveilig jouw scherm bij het kortstondig verlaten van het toestel, stel eventueel een automatische schermvergrendeling in
- sluit programma's en computers / laptops af op het einde van een werkdag
- gegevenslekken moeten gemeld worden bij de ICT-coördinator en directie (moedwillig stelen, verlies of diefstal, technisch falen, …)

Art.12 Het personeelslid sluit dagelijks na gebruik zijn PC af zodat de back-up van de bestanden veilig kan worden genomen.

Art.13 <u>Virussen</u>

§1 Het personeelslid moet de geïnstalleerde beveiligingssoftware gebruiken en alle richtlijnen in dit verband opvolgen. Het personeelslid mag de beveiligingssoftware niet wijzigen of uitschakelen.

§2 Bij het gebruik van eigen opslagmedia (diskettes, cd-roms, dvd's, memorysticks,…) op de ICT-infrastructuur van de onderwijsinstelling, moeten deze vooraf gescand worden op virussen.

§3 Het personeelslid mag nooit zelf proberen virussen te vernietigen.

Art.14 De ICT-coördinator en/of functionaris gegevensbescherming moet zo snel mogelijk op de hoogte worden gebracht bij elk incident in verband met de veiligheid of elke ontdekte tekortkoming in de beveiliging van de ICT-infrastructuur waardoor de vertrouwelijkheid, de integriteit en/of de beschikbaarheid van de informatie of het informatiesysteem in het gedrang kunnen komen. In dat geval is het personeelslid tot geheimhouding tegenover anderen gebonden.

Art.15 Het schoolbestuur of zijn afgevaardigde kan de toegang tot (bepaalde) websites verhinderen.

Art.16 Met het oog op de continuïteit van de dienstverlening kan de directeur in geval van overmacht of in uitzonderlijke omstandigheden informatie, systemen, bestanden of gegevens die essentieel zijn en die niet langer op een andere wijze beschikbaar zijn, laten lokaliseren en recupereren.

Hoofdstuk 4 Beroepsmatig en persoonlijk gebruik

Art.17 Beroepsmatig gebruik

Het personeelslid kan binnen de grenzen van deze policy vrij gebruik maken van de ICT-infrastructuur die hem ter beschikking is gesteld in functie van de uitvoering van de opdrachten die hem door het schoolbestuur of de directeur zijn toevertrouwd.

Art.18 Persoonlijk gebruik

De ICT-infrastructuur kan beperkt en occasioneel voor privédoeleinden gebruikt worden voor zover:

- dit gebeurt buiten de werkuren van het personeelslid;
- het personeel dat nog of reeds aan het werk is, niet wordt gestoord;
- persoonlijke bestanden of gescande files niet opgeslagen worden op de ICT-infrastructuur van de onderwijsinstelling;
- privémail zo snel mogelijk wordt gewist;
- dit geen gevolg heeft voor de goede werking van het netwerk.

Art.19 Indien het personeelslid van artikel 18 gebruik maakt voor privécommunicatie per e-mail, dan moet hij elke vermelding met betrekking tot de onderwijsinstelling weglaten en elke aanduiding vermijden die de indruk zou kunnen wekken dat het bericht onder het toezicht van of met goedkeuring van de onderwijsinstelling of het schoolbestuur werd opgesteld of verzonden.

Art.20 Het personeelslid doet alle mogelijke inspanningen om te vermijden dat er privémails door derden aan hem worden gericht.

Hoofdstuk 5 Gebruik van internet en sociale media

Art.21 De school heeft een website en facebook-account.
Deze kanalen bieden de mogelijkheid om te laten zien dat je trots bent op je werk en kunnen een bijdrage leveren aan een positief imago van de school. Desalniettemin is het belangrijk te beseffen dat je met berichten op internet en sociale media (onbewust) het imago van de school ook kunt schaden. Het schoolbestuur vertrouwt erop dat zijn medewerkers deontologisch verantwoord zullen omgaan met internet en sociale media.

- De leerkrachten mogen artikelen en foto's publiceren op de websitepagina van hun klas. Ze doen dit op een deontologisch verantwoorde manier. Ze houden daarbij privé en werk gescheiden.
- De personeelsleden dienen zich ervan bewust te zijn dat de gepubliceerde inhoud voor onbepaalde tijd openbaar zal zijn, ook na verwijdering van het bericht.
- Er mogen geen online discussies over de school gevoerd worden op internet en sociale media.
- Bij twijfel of een publicatie deze richtlijnen schaadt neemt de leerkracht contact op met de directie.

Het is niet toegestaan om werk gerelateerde gegevens (persoonsgegevens, foto's, … van zowel leerlingen of collega's) op persoonlijke sociale media te posten.

Hoofdstuk 6 Gebruik van foto's en afbeeldingen

Het gebruik van allerlei vormen van beeldmateriaal (bv. foto, film, dvd, internet, e-letters, gsm, ...) evolueert razendsnel.

Art.22 Eigen foto's, bewegende beelden

- vooraleer je een foto / film neemt van iemand, moet je hem om zijn toestemming vragen
- wil je nadien deze foto's / films publiceren op onze website, facebookpagina of in een folder, infoblad, pers ...dan moet je hiervoor nogmaals zijn toestemming vragen
- voor gebruik van de foto's voor schoolse activiteiten (knutselen, herkenningswerken,...) moet vooraf toestemming gegeven worden
- een minderjarige kan zelf geen toestemming geven. In dit geval moeten de ouders dus toestemming geven. Hiervoor verwijzen we naar de toestemmingsformulieren welke door de ouders bij de inschrijving worden ingevuld. Deze gegevens kan je ook raadplegen in Broekx-on-web bij leerlingfiche (vrije velden). Het is belangrijk om de keuzes van het toestemmingsformulier steeds te respecteren! Indien je foto's of andere gegevens voor andere doeleinden, dan vermeld op het toestemmingsformulier wil gebruiken, moet je daarvoor apart toestemming vragen. Gelieve dan contact op te nemen met de directie.

Art.23 Bestaande foto's, afbeeldingen, bewegende beelden

- vóór je de beelden gebruikt, moet je natuurlijk ook steeds nagaan of sommige daarvan niet auteursrechtelijk beschermd zijn (het zogenaamde "copyright")
- gebruik daarom eigen foto's (met toestemming) of foto's van een databank waar je (gratis) licentievrije foto's kan downloaden. Enkele voorbeelden van websites:
    - www.shutterstock.com/nl (betalend)
    - http://pixabay.com/nl/
    - www.freepik.com
    - www.splitshire.com
    - www.dreamstime.com
    - http://nl.123rf.com/
- gebruik je beeldmateriaal van een fotograaf, filmmaker, ... vermeld dan zeker altijd je bron.

Wat zijn de regels na 25 mei 2018 wanneer de nieuwe privacywet van kracht gaat? Op de website van Kortom vind je een overzicht:
https://www.kortom.be/nieuws/8258/fotos-en-gdpr-wat-zijn-de-nieuwe-regels

Hoofdstuk 7 Hoe omgaan met persoonsgegevens?

Vanaf 25 mei 2018 zijn de privacyregels aanzienlijk veranderd door de invoering van de Europese GDPR-wetgeving (Algemene Verordening Gegevensbescherming), om zo de burger te beschermen rond gebruik van persoonsgegevens. Elke organisatie die persoonsgegevens verwerkt, moet dat volgens deze regels doen. De regels roepen vragen op: Wat kan/moet ik doen om privacygegevens te beschermen? Wat met mailings? Wat met de lijsten met persoonsgegevens?

Wat zijn persoonsgegevens?

- naam

- foto
- adres
- telefoonnummer (ook nummer op het werk)
- geheime codes (toegangscode, paswoord …)
- bankrekeningnummer
- rijksregisternummer
- e-mailadres(sen)
- vingerafdruk
- …

Art.24 Neem volgende richtlijnen in acht:

- stuur geen mails, nieuwsbrieven of andere informatie tenzij je uitdrukkelijke toestemming hebt van de geadresseerde;
- indien je een groep personen mailt, zorg er dan voor dat ze elkaars e-mailadressen niet zien (gebruik BCC);
- let op de inhoud van een ontvangen e-mail voordat je deze doorstuurt (misschien bevat deze persoonsgegevens die niet zomaar mogen worden doorgegeven);
- vraag geen overbodige persoonsgegevens op voor je dienstverlening (geen adres, rijksregisternummer, …) wanneer je eigenlijk alleen de telefoonnummer zal gebruiken;
- geef zeker geen persoonsgegevens door aan derden, tenzij het over een wettelijke verplichting gaat of je uitdrukkelijke toestemming hebt gekregen van de betrokkene
- indien je lijsten aanmaakt die persoonsgegevens bevatten, contacteer dan Carl Sledsens zodat hier de nodige documenten voor worden ingevuld;
- verwijder persoonsgegevens van bovenstaande lijst van zodra je deze niet meer nodig hebt
- laat geen papieren met persoonsgegevens rondslingeren in de school
- hang geen papieren met persoonsgegeven op in de gangen, klassen, refter,…
- haal je afdrukken op de centrale printer direct af, laat deze niet onbewaakt liggen op de printer
- mocht je toch dergelijke papieren tegenkomen, die niet voor jou bedoeld zijn, bezorg deze dan aan de verwerker
- versnipper papieren met persoonsgegevens die je niet meer nodig hebt, gooi deze in geen geval zomaar in de papiermand
- mocht je foto's maken, vraag dan altijd toestemming om 1) de foto te maken en 2) om deze te mogen gebruiken in een publicatie, op de website, sociale media, …; Hiervoor verwijzen we naar de toestemmingsformulieren welke door de ouders bij inschrijving worden ingevuld. Deze gegevens kan je ook raadplegen in Broekx-on-web bij leerlingfiche (vrije velden).
- neem geen persoonsgegevens op in klaslijsten en hang ze niet op zonder dat je daarvoor de uitdrukkelijke toestemming van de ouders hebt gekregen.
- indien een ouder vragen heeft in verband met privacy, mag je deze doorverwijzen naar de directie of naar privacy@kasterlee.be

Hoofdstuk 8 Verboden

Art.25 Zonder limitatief te zijn, mag de ICT-infrastructuur van de onderwijsinstelling nooit (noch beroepsmatig, noch bij persoonlijk gebruik) gebruikt worden voor volgende zaken:

§1 om informatie te verkrijgen, te verwerken, te verspreiden of op te slaan in strijd met de regelgeving, in het bijzonder (niet-limitatieve opsomming):
- de wetgeving op de bescherming van de persoonlijke levenssfeer,

- de wetgeving in het domein van de telecommunicatie
- de wetgeving over de handelspraktijken die betrekking hebben op commerciële communicatie;
- de wetgeving over het auteursrecht en andere intellectuele rechten;
- de wetgeving ter bestrijding van het racisme of informatie die in het algemeen beledigend of lasterlijk is voor andere personen;
- de wetgeving over de bescherming van de goede zeden (informatie die een pornografisch of uitgesproken erotisch karakter heeft);

§2 om acties te ondernemen die de beveiliging van systemen of informatie in het gedrang kunnen brengen, zoals bijvoorbeeld:
- interne en externe systeem- en netwerkbeveiliging omzeilen,
- schadelijke software (bijvoorbeeld programma's besmet met virussen) creëren of op de computers van de onderwijsinstelling introduceren,
- zich toegang verschaffen tot systemen of informatie waartoe men niet geautoriseerd is;
- toegang tot het netwerk verschaffen aan personen die hiertoe niet geautoriseerd zijn, behoudens in opdracht van het schoolbestuur of zijn afgevaardigde;
- een valse identiteit aannemen;
- bestanden van andere personeelsleden verwijderen of wijzigen, behoudens expliciete toestemming;
- downloaden, kopiëren en installeren van software zonder toestemming van het schoolbestuur of zijn afgevaardigde;
- programma's gebruiken in strijd met de licentievoorwaarden;
- de structuur of de configuratie van de ICT-infrastructuur wijzigen zonder toestemming van het schoolbestuur of zijn afgevaardigde;

§3 om informatie te verkrijgen, te verwerken, te verspreiden of op te slaan die:
- schadelijk kan zijn voor de onderwijsinstelling, het gemeentebestuur of het imago ervan;
- vertrouwelijk is of die wegens de aard ervan redelijkerwijze als vertrouwelijk moet worden beschouwd, tenzij men die informatie in het kader van de toegewezen opdracht moet behandelen en dit niet indruist tegen de regelgeving;
- hinderlijk is voor anderen zoals aan grote groepen van gebruikers ongewenste berichten verspreiden, lasterlijke feiten verspreiden of onware en geringschatte informatie verspreiden;
- aanstootgevend is voor anderen omdat ze tegen de algemeen geldende fatsoenregels indruist;

§4 om deel te nemen aan kansspelen of loterijen;

§5 in het kader van een zelfstandige activiteit van het personeelslid;

§6 voor politieke activiteiten of doeleinden.

Art.26 Zonder limitatief te zijn, mag de ICT-infrastructuur van de onderwijsinstelling voor de volgende zaken enkel gebruikt worden als dit gebeurt in functie van de uitvoering van de opdracht van het personeelslid:
- om muziek-, radio- of televisieprogramma's te beluisteren/bekijken via het internet;
- om deel te nemen aan chatrooms of newsgroups;
- voor het spelen van computerspelletjes;
- voor zaken met winstgevend doel.

Hoofdstuk 9 Controle

Art.27 De algemeen directeur, de directeur, de ICT-coördinator en de functionaris gegevensbescherming waken over de naleving van dit reglement.

Art.28 Het schoolbestuur kan het gebruik van internet, e-mail en andere communicatiemiddelen permanent of tijdelijk laten controleren. Dit gebeurt desgevallend met eerbiediging van de regelen van de privacy.

Art.29

§1 Controle op het communicatiegebruik gebeurt enkel met het oog op:

- het voorkomen van ongeoorloofde of lasterlijke feiten, feiten die strijdig zijn met de goede zeden of die de waardigheid van een andere persoon kunnen schaden;
- de veiligheid en/of de goede technische werking van het ICT-netwerksysteem, met inbegrip van de controle op de kosten die ermee gepaard gaan, alsook de fysieke bescherming van de installaties van de onderwijsinstelling;
- het te goeder trouw naleven van de regels rond gebruik van ICT-middelen zoals vermeld in onderhavige policy (en eventueel in het arbeidsreglement).

§2 Het schoolbestuur zal in zijn controle niet verder gaan dan nodig is voor het verwezenlijken van deze doelstellingen. Ze kiest de controlemethode die de geringst mogelijke inmenging in de persoonlijke levenssfeer van het personeelslid tot gevolg heeft.

Art.30 Het schoolbestuur kan een algemene lijst van de elektronische onlinecommunicatie-gegevens bijhouden. De resultaten worden elektronisch geregistreerd en bijgehouden gedurende een periode van vier maanden. Nadien worden ze verwijderd, tenzij zij het voorwerp uitmaken van een onderzoek.

Art.31 Indien ernstige vermoedens ontstaan van misbruik of onregelmatigheden, dan kan de algemeen directeur de elektronische onlinecommunicatiegegevens verwerken om ze aan een geïdentificeerde of identificeerbare persoon toe te schrijven.

Art.32 Gegevens of communicatie waarvan niet uitdrukkelijk is aangegeven dat het gaat om privé-informatie, kunnen op elk moment door de directeur of de algemeen directeur worden ingekeken.

Art.33 Privécommunicaties kunnen bij ernstig vermoeden van misbruik of van niet-naleving van de policy gecontroleerd worden op hun aantal, tijdstip en/of hun inhoud in het bijzijn van de betrokken gebruiker.

Art.34 Het resultaat van de controle zal ter kennis van het personeelslid worden gebracht.

Hoofdstuk 10 Sancties

Art.35 Het personeelslid kan aansprakelijk gesteld worden voor alle schade die hij opzettelijk heeft toegebracht of die voortvloeit uit het onvoorzichtig omspringen met zijn gebruikersnaam, wachtwoord of andere beveiligingsinformatie.

Art.36 Het schoolbestuur of zijn afgevaardigde kan de toegang tot ICT-infrastructuur geheel of gedeeltelijk intrekken bij een overtreding van deze policy of van andere onderrichtingen.

Art.37 Het schoolbestuur of zijn afgevaardigde kan te allen tijde de toelating tot privégebruik geheel of gedeeltelijk intrekken.

Art.38 Andere sancties kunnen worden opgelegd conform het arbeidsreglement.

Hoofdstuk 11 Contactpersonen

Algemeen directeur gemeente Kasterlee
Tom De Munter, tom.demunter@kasterlee.be

Functionaris gegevensbescherming gemeente Kasterlee
Jef Van Bylen, jef.vanbeylen@iok.be

Directeur GBS De Pagadder
Anne Meeus, directie@gbsdepagadder.be

Directeur GBS De Vlieger
Viviane Wouters, directie@gbsdevlieger.be

Aanspreekpunt informatieveiligheid
Carl Sledsens, carl.sledsens@kasterlee.be