COMMUNICATIEBELEID

VZW KOGA

voor:

Sint-Lievenscollege Humaniora SO (127696 en 127688)

Sint-Lievenscollege Business SO (036913)

Sint-Janscollege SO (115361 en 115352)

internaat Sint-Lievenscollege Humaniora en Business (115246 en 101477)

Deze nota maakt deel uit van het informatieveiligheid- en privacybeleid (IVPB).

Versie	Datum	Status	Auteur(s)	Opmerking
1.0	2018-05-25	GELDIG	Cocquyt Vanessa	

1 Inleiding

De manier waarop personeelsleden, en ook leerlingen en ouders, communiceren maakt ook een deel uit van het IVP-beleid. In dit document worden enkele principes vastgelegd inzake interne én externe communicatie, teneinde er samen voor te zorgen dat de privacy, de informatieveiligheid op en het imago van VZW KOGA op een gepast niveau wordt behouden.

Deze nota valt onder de eindverantwoordelijkheid van VZW KOGA.

2 Discretieplicht

Alle personeelsleden van VZW KOGA zijn gebonden aan een **discretieplicht**, ten aanzien van de persoonsgegevens van leerlingen, ouders of het gezin, en eventueel ten aanzien van elkaars persoonsgegevens. In het *algemeen reglement van het personeel van het katholiek onderwijs* (art. 7 § 7, art. 23 § 1) wordt hiernaar verwezen.

Dit betekent concreet dat zij van ambtswege uit, geen persoonsinformatie mogen vermelden of publiceren, buiten de daarvoor voorziene kanalen binnen VZW KOGA. Onderling informatie delen mag natuurlijk, maar dan via de hieronder vastgelegde kanalen en procedures, en steeds indien het in het belang is van het kind, de kinderen of eventueel de collega in kwestie.

Personeelsleden worden dus van ambtswege uit geacht om de geldende beveiligings- en privacyprocedures en -afspraken steeds te volgen, teneinde het **accidenteel** verspreiden van persoonsgegevens te vermijden. Indien men vermoedt dat, door toedoen van uzelf of van anderen, er mogelijks persoonsgegevens buiten de context van deze discretieplicht “geraakt” zijn, dan dient men het aanspreekpunt informatieveiligheid en/of het meldpunt datalekken hierover te contacteren.

Voor VZW KOGA is het meldpunt datalekken: privacy@vzwkoga.be.

3 E-mailbeleid

Voor personeelsleden wordt hiernaar verwezen in het *algemeen model van arbeidsreglement, opgesteld door Katholiek Onderwijs Vlaanderen*.

Op VZW KOGA maken we onderscheid tussen drie categorieën van e-mailaccounts:

- Algemene schoole-mail (zoals o.a. *info@instelling.be*, *directie@instelling.be*, *leerkrachten@instelling.be*, …)
- Privé-e-mail (zelf aangemaakt Gmail, Outlook, Live, Yahoo, … account)
- Persoonlijke school- of werk-email (van de vorm *voornaam.naam@instelling.be*)

Voor elk van deze categorieën leggen we in deze paragraaf een aantal richtlijnen / afspraken vast inzake het doel, gebruik én de beveiliging van de accounts in kwestie.

Algemene opmerking: *Verzend nooit een wachtwoord, voor eender welk platform, via email of een ander communicatiesysteem. Niemand van VZW KOGA zal op deze manier ooit een wachtwoord opvragen.*

3.1 Algemene accounts

Het beheer hiervan is toegewezen aan één of meerdere medewerkers.

Deze adressen worden vrij verspreid en gepubliceerd.

Indien het adres verwijst naar een groep van personen, dan dient men het steeds in “blind carbon copy” (BCC) te plaatsen.

3.2 Privé accounts

Deze accounts worden bij voorkeur gebruikt voor niet-school gerelateerde communicatie of handelingen.

Deze adressen worden niet verspreid of gepubliceerd. Ze worden enkel intern gebruikt door directie, administratie of op eigen initiatief.

Het gebruik van dergelijke accounts is niet verboden op VZW KOGA, zolang het de professionele bezigheden niet hindert en de informatieveiligheid niet in het gedrang komt.

Concreet:

- Het is niet toegestaan om berichten te verzenden met een pornografische, racistische, discriminerende, beledigende of aanstootgevende inhoud.
- Het is niet toegestaan om berichten te verzenden met een (seksueel) intimiderende inhoud.
- Het is niet toegestaan om berichten te verzenden die (kunnen) aanzetten tot haat en/of geweld.

Gebruik geen privé accounts voor communicatie met collega's aangaande instellingsgebonden zaken of voor de communicatie met leerlingen, oud-leerlingen, ouders of externen (zie § 3.3).

Let er bij het gebruik van privé accounts, op toestellen of een netwerk waarop zich ook persoonsgegevens van VZW KOGA bevinden, op dat bijlagen, hyperlinks, tools, … die met de privé accounts gebruikt worden, niet leiden tot beveiligingsgevaren zoals virussen, ransomware, phishing[1] enz.

3.3 Schoolaccounts (werkadressen)

Deze zijn telkens toegewezen aan één medewerker en zijn identificeerbaar voor die functie / medewerker.

Deze adressen kunnen verspreid en gepubliceerd worden.

Gebruik deze accounts voor communicatie met collega's aangaande instellingsgebonden zaken of voor de communicatie met leerlingen, oud-leerlingen, ouders of externen.

Natuurlijk gelden dezelfde afspraken voor deze accounts als voor privéaccounts:

- Deze accounts worden aan de medewerker voor professioneel gebruik beschikbaar gesteld. Gebruik is derhalve verbonden met taken die voortvloeien uit de functie.
- Beperkt persoonlijk gebruik van deze accounts is evenwel toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden en dit geen verboden gebruik in de zin van § 3.2 oplevert:

- Het is niet toegestaan om berichten te verzenden met een pornografische, racistische, discriminerende, beledigende of aanstootgevende inhoud
- Het is niet toegestaan om berichten te verzenden met een (seksueel) intimiderende inhoud.
- Het is niet toegestaan om berichten te verzenden die (kunnen) aanzetten tot haat en/of geweld.

Bijkomende afspraken:

- Verzend bij voorkeur **geen gevoelige persoonsgegevens** over leerlingen via deze accounts, of via eender welk ander berichtensysteem (zie ook § 4).
  Dit maakt het voor de verantwoordelijken onmogelijk om iedereens privacy en/of de informatieveiligheid als geheel te waarborgen. Mogelijks leidt dit er toe dat VZW KOGA niet alle rechten en vrijheden van leerlingen, ouders of medewerkers kan waarborgen.
  Met gevoelige informatie bedoelen we o.a. gezinssituatie, psycho-sociaal, medisch, zorg, financieel.
  Gebruik het (centraal beheerde en beveiligde) leerlingvolgsysteem om deze informatie met de juiste collega's en medewerkers te delen.
- Indien u via dit emailaccount (gevoelige) persoonsgegevens ontvangt, plaats deze dan zo snel mogelijk in het **(centraal beheerde en beveiligde) leerlingvolgsysteem** of laat een bevoegde medewerker dit er in plaatsen.
  Verwijder daarna alle berichten die deze gegevens bevatten of behandelden (ook uit uw "Prullenmand").
- Gebruik dit account niet voor platformen die niet nodig zijn om uw taak voor VZW KOGA uit te voeren of voor platformen **die niet "informatieveilig" beschouwd worden** door het aanspreekpunt informatieveiligheid. Contacteer voor vragen hierrond privacy@vzwkoga.be.
- Maak zo veel mogelijk gebruik van "blind carbon copy" (BCC) indien u met meerdere mensen communiceert.
- Let op wie u bij de ontvangers plaatst of in kopieert, met "carbon copy" (CC).

[1] Meer informatie over "phishing" is te vinden in § 1 van de ***achtergrondinformatie***.

4 Beleid inzake communicatie-apps

Naast email, zijn er tegenwoordig tal van andere communicatieplatformen, ook op mobiele toestellen. Op VZW KOGA moedigen we het (professionele, correcte) gebruik van allerhande tools, platformen en apps natuurlijk aan, maar tegelijkertijd willen we iedereen wijzen op het correcte gebruik ervan, en i.h.b. ten aanzien van privacy-gevoelige informatie.

We menen dat medewerkers, ouders en leerlingen verbonden aan VZW KOGA hoofdzakelijk een of meerdere van de volgende communicatieplatformen gebruiken:

- Het berichtensysteem van Smartschool
- Instant messaging via telefonie, zoals bv. SMS, MMS e.d.
- Instant messaging online, zoals bv. Messenger, WhatsApp, Google Hangouts, …
- Video conferencing, zoals bv. Skype, FaceTime, Google Hangouts, …

4.1 Intern berichtensysteem

Voor het beleid en de regels rond het **interne berichtensysteem**, verwijzen we naar het gebruik van de school email-accounts, zoals beschreven in § 3.3.[2]

Indien Smartschool een “app” aanbiedt om het interne communicatiesysteem (en eventueel andere functionaliteiten of modules) te raadplegen op een mobiel toestel, verplichten wij om dit toestel met een vergrendeling te beveiligen (zie § 5.2 in het ***toestelbeleid***).

4.2 Instant messaging

Deze communicatiekanalen kunnen heel zinvol zijn, ook voor een snel (informeel) werkoverleg, maar binnen VZW KOGA is het ten strengste afgeraden om persoonsgegevens van leerlingen te communiceren via een van deze kanalen.

Indien deze kanalen en/of school emailaccounts geraadpleegd worden op een mobiel toestel, vragen wij om dit toestel met een vergrendeling te beveiligen (zie § 5.2 in het ***toestelbeleid***).

4.3 Video conferencing

Ook deze tools zijn zeer interessant, bv. om een overleg van op afstand of met een anders verhinderde collega uit te voeren, maar wees u bewust van:

- de mogelijkheid om in deze tools stem- en/of video-opnames te maken;
- de mogelijkheid om een scherm te delen / over te nemen.

Indien de video conferencing een “app” gebruikt op een mobiel toestel, vragen wij om dit toestel met een vergrendeling te beveiligen (zie § 5.2 in het ***toestelbeleid***).

[2] We wijzen er iedereen via deze weg op dat de beheerders van Smartschool de berichtinhoud van andere gebruikers onmogelijk kunnen lezen.

5 Social Media-protocol

Bron: https://www.hetstreek.nl/sites/default/files/Protocol%20Sociale%20Media%20%20-%20april%202012.pdf

5.1 Inleiding

Sociale media zoals Twitter, Facebook, LinkedIn, Instagram, Snapchat, … en nog vele anderen bieden de mogelijkheid te laten zien dat men trots is op de school. Tevens kunnen ze een bijdrage leveren aan een positief imago van VZW KOGA.

Het is daarbij van belang te beseffen dat berichten op sociale media (onbewust) de goede naam van de school en betrokkenen ook kunnen schaden. Om deze reden vraagt VZW KOGA de aan de school verbonden personen om verantwoord met sociale media om te gaan, de reguliere fatsoensnormen in acht te nemen en de mogelijkheden met een positieve instelling te benaderen.

VZW KOGA heeft dit protocol opgezet om aan iedereen die betrokken is, of zich betrokken voelt, richtlijnen te geven. Deze richtlijnen maken een effectieve inzet van sociale media mogelijk. VZW KOGA is zich bewust van het feit dat de mogelijkheden van sociale media omvangrijk zijn en dat ze bijna dagelijks veranderen. Om enige toekomstvastheid van dit protocol te borgen zijn de richtlijnen zo generiek als mogelijk omschreven, maar wel getoetst op toepasbaarheid in specifieke situaties.

5.2 Uitgangspunten

1. VZW KOGA onderkent het belang van sociale media.

2. Dit protocol heeft als doel bij te dragen aan een goed en veilig school- en onderwijsklimaat.

3. Dit protocol bevordert dat indien de school, medewerkers, leerlingen en ouders op de sociale media communiceren, dit gebeurt in het verlengde van de missie en visie van de onderwijsinstelling en de reguliere fatsoensnormen. In de regel betekent dit dat we zorgvuldig communiceren, respect voor de school en voor elkaar hebben en iedereen in zijn waarde laten.

4. Het protocol heeft als doel de onderwijsinstelling, de medewerkers, de leerlingen en de ouders te beschermen tegen de mogelijk negatieve gevolgen van sociale media.

5.3 Doelgroep en reikwijdte

Deze richtlijnen zijn bedoeld voor alle betrokkenen die deel uitmaken van de “schoolomgeving”, dat wil zeggen medewerkers, leerlingen, ouders/verzorgers en mensen die op een andere manier verbonden zijn aan VZW KOGA.

De richtlijnen in dit protocol hebben betrekking op alle op enigerlei wijze aan school of haar medewerkers te relateren berichten.

5.4 Sociale media in de school

5.4.1 *Voor alle gebruikers*

1. Het is leerlingen niet toegestaan om tijdens de lessen actief te zijn op sociale media tenzij er op voorhand door de schoolleiding, leraren en/of onderwijsondersteunend personeel toestemming is gegeven.

2. Het is medewerkers toegestaan om tijdens de lessen actief te zijn op sociale media zolang dit een onderwijskundige doelstelling heeft.

3. Het is betrokkenen toegestaan om kennis en informatie te delen, mits het geen vertrouwelijke informatie betreft en andere betrokkenen niet schaadt.

4. De betrokkene is persoonlijk verantwoordelijk voor de inhoud welke hij of zij publiceert op de sociale media.

5. Elke betrokkene dient zich ervan bewust te zijn dat de gepubliceerde teksten en uitlatingen voor onbepaalde tijd openbaar zullen zijn en kunnen blijven, ook na verwijdering van het bericht. Dat vraagt om extra zorg en enig voorbehoud bij het plaatsen van berichten.

6. Het is niet toegestaan om foto-, film- en geluidsopnamen van school gerelateerde situaties op de sociale media te zetten tenzij de betrokkenen hier uitdrukkelijk toestemming voor hebben gegeven.

7. Op de sociale media waarop geen volledige controle mogelijk is op de berichten die er door anderen worden geplaatst (zoals bv. Facebook) is het medewerkers van VZW KOGA afgeraden om privé pagina's en uitingen te delen of het zogenaamde 'vrienden' worden met leerlingen van VZW KOGA. De communicatie op deze sociale media vindt plaats via generieke pagina's en profielen (Zie § 5.4.2).

5.4.2 *Voor medewerkers in werksituaties*

1. Indien het wenselijk is dat er voor een bepaald doel een pagina op sociale media wordt aangemaakt, dan wordt hiervoor een generiek, duidelijk aan school gebonden profiel gebruikt. Het aanmaken van een dergelijke pagina wordt op voorhand met de directe leidinggevende besproken.

2. Elke betrokkene is zich bewust van het feit dat (op sommige sociale media) ook anderen informatie kunnen plaatsen op (profiel) pagina's (taggen, linken, posten, etc.).

3. Om die reden zal de eigenaar van de pagina (of topic, discussie, etc.) controlerend optreden en actief redactie voeren op de onder zijn of haar verantwoording aangemaakte pagina's. Zodra de pagina's niet meer nodig zijn worden deze ook door hem of haar weer verwijderd of op non actief gesteld.

4. Medewerkers hebben een bijzondere verantwoordelijkheid bij het gebruik van sociale media. Wanneer een medewerker deelneemt aan een discussie of informatie plaatst op een generieke aan school gebonden pagina, dan dient dit in overeenstemming met de officiële standpunten, missie en visie van de onderwijsinstelling te geschieden.

5. Als online communicatie dreigt te ontsporen dient de medewerker direct contact op te nemen met zijn/haar leidinggevende om de te volgen strategie te bespreken.

6. Bij twijfel of een publicatie in strijd is met deze richtlijnen neemt de medewerker contact op met zijn/haar leidinggevende.

5.4.3 *Voor medewerkers buiten werksituaties*

1. Het is medewerkers toegestaan om persoonlijke webpagina's, weblogs, vlogs enz. te onderhouden. Het is daarbij niet toegestaan om aan school gerelateerde onderwerpen te publiceren voor zover het vertrouwelijke of persoonsgebonden informatie over de school, zijn medewerkers, leerlingen, ouders/verzorgers en andere betrokkenen betreft. Een medewerker kan steeds aangesproken worden op berichten, geplaatst op sociale media. Medewerkers moeten zich bewust zijn van hun voorbeeldfunctie.