COMMUNICATIEBELEID

vzw Onderwijsinrichting van de Ursulinen te Onze-Lieve-Vrouw-Waver

voor:

Sint-Ursula-Instituut (instellingsnummers 126946, 126953, 126961)

Bosstraat 9

2861 Onze-Lieve-Vrouw-Waver

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

Versie	Datum	Status	Auteur(s)	Opmerking
1.0	2018-05-25	GELDIG	A. Vanhaeren, AIV	

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 het Sint-Ursula-Instituut op een gepast niveau worden behouden.

Deze nota valt onder de eindverantwoordelijkheid van vzw Onderwijsinrichting van de Ursulinen te O.-L.-V.-Waver.

2 Discretieplicht

Alle personeelsleden van het Sint-Ursula-Instituut 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 het Sint-Ursula-Instituut. 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 het Sint-Ursula-Instituut is het meldpunt datalekken: ***privacy@sui.be***.

3 E-mailbeleid

Voor personeelsleden wordt hiernaar verwezen in het algemeen model van arbeidsreglement (bijlage 3, punt 3.5).

In het Sint-Ursula-Instituut maken we onderscheid tussen drie categorieën van e-mailaccounts:

- Algemene schoole-mail (zoals o.a. *info@sui.be*, *afwezig@sui.be, ict@sui.be*…)
- Privé e-mail (zelf aangemaakt Gmail, Outlook, Live, Yahoo, … account)
- Persoonlijke school- of werke-mail (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 e-mail of een ander communicatiesysteem. Niemand van het Sint-Ursula-Instituut 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 in het Sint-Ursula-Instituut, 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.

Let er bij het gebruik van privé accounts, op toestellen of een netwerk waarop zich ook persoonsgegevens van het Sint-Ursula-Instituut 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 privé accounts:

- 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 ieders privacy en/of de informatieveiligheid als geheel te waarborgen. Mogelijks leidt dit er toe dat het Sint-Ursula-Instituut 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 e-mailaccount (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 op het world wide web, voor platformen die niet nodig zijn om uw taak voor het Sint-Ursula-Instituut uit te voeren of voor platformen **die niet "informatieveilig" beschouwd worden** door het aanspreekpunt informatieveiligheid. Contacteer voor vragen hierrond *privacy@sui.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).

4 Beleid inzake communicatie-apps

Naast e-mail, zijn er tegenwoordig tal van andere communicatieplatformen, ook op mobiele toestellen. In het Sint-Ursula-Instituut moedigen we het (professionele, correcte) gebruik van allerhande tools, platformen en apps

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

natuurlijk aan, maar tegelijkertijd willen we iedereen wijzen op het correcte gebruik ervan, en in het bijzonder ten aanzien van privacygevoelige informatie.

We menen dat medewerkers, ouders en leerlingen verbonden aan het Sint-Ursula-Instituut hoofdzakelijk één of meerdere van de volgende communicatieplatformen gebruiken:

- een mailsysteem zoals Outlook...;
- 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 e-mail-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, vragen 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 het Sint-Ursula-Instituut is het ten strengste afgeraden om persoonsgegevens van leerlingen te communiceren via één van deze kanalen.

Indien deze kanalen en/of school e-mailaccounts 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.