Policy Omgaan met e-mail

Informatieveiligheid – Omgaan met e-mail

1. Doel

Deze policy heeft als doel ervoor te zorgen dat het e-mailsysteem binnen het CLB op een correcte manier wordt gebruikt en dat de gebruikers ervan bewust zijn van wat de organisatie als aanvaardbaar, respectievelijk onaanvaardbaar gebruik van e-mail beschouwt.

2. Verantwoordelijkheden en bevoegdheden

Alle personeelsleden zijn bevoegd om e-mail te gebruiken en zijn verantwoordelijk voor het correct omgaan met mail.

3. Toepassingsgebied

Deze policy is van toepassing op alle personeelsleden van het CLB.

4. Middelen

E-mail-software: …………(vb. Outlook, Google,...)

E-mail-infrastructuur: ………. (vb. Exchange Server, Google Apps for Education,...)

5. Referenties

• Policy Omgaan met wachtwoorden

• Procedure Incidentmelding

• Werkinstructie Beheer e-mail

Besluit van de Vlaamse Regering betreffende het multidisciplinaire dossier in de centra voor leerlingenbegeleiding van 12 september 2008, B.S.17/11/2008, Laatste wijziging 05/10/2016

• Algemene policy inzake gebruik van e-mail, versie 0.30, 23/06/2010, werkgroep Informatieveiligheid van de Kruispuntbank van de Sociale Zekerheid.

6. Werkwijze

E-mail wordt gebruikt als een professioneel communicatiemiddel. Daarom is het belangrijk dat gebruikers er zich bewust van zijn dat ze e-mail op een correcte, verantwoorde en veilige manier moeten gebruiken.

6.1. Algemene richtlijnen

• Elke medewerker van het CLB krijgt een mailaccount. Om toegang tot e-mail te bekomen, verstrekt het CLB de gebruiker een e-mailadres, gebruikersnaam en wachtwoord. Gebruik voor het versturen van mails steeds je eigen account. Ga daarbij op een verantwoorde manier om met je wachtwoord (zie policy rond wachtwoorden).

• Behandel professionele mails steeds in de aangeboden mailprogramma’s van het CLB. Verstuur professionele mails steeds vanuit je CLB-mailadres. Stuur ze niet door naar een eigen, externe mailbox of derden (zonder voorafgaandelijke afspraken/toestemming) aangezien deze overdracht de vertrouwelijkheid van de gegevens in gevaar zou kunnen brengen.

* Verstuur nooit gevoelige informatie door via email. Gevoelige informatie kan slechts d.m.v. versleuteling verstuurd worden via email.
* Communiceer steeds op een correcte manier.
* Stuur neutrale berichten conform uw deontologische code
* Om overvolle mailboxen te vermijden, vragen we iedereen op een verantwoorde en efficiënte manier om te gaan met mail. Verkies persoonlijk contact of de telefoon boven mail, zeker voor dringende zaken.
* Wees zuinig met CC, BCC, allen beantwoorden. Stuur het bericht enkel naar die personen die echt op de hoogte moeten zijn of expliciet om een kopie gevraagd hebben. Gebruik BCC indien geadresseerden elkaars contactgegevens niet mogen kennen.
* Om de authenticiteit van je mails te garanderen, gebruik je best een digitale handtekening.
* Voeg een disclaimer toe.

6.2. Professioneel versus persoonlijk gebruik

Het gebruik van de elektronische communicatiemiddelen die ter beschikking gesteld worden door het CLB, is bedoeld voor professionele doeleinden.

Indien het CLB je toelaat privé-mails te versturen of te ontvangen met je professionele account, worden deze na lezen onmiddellijk verwijderd of in een map ‘Privé’ of ‘Persoonlijk’ geklasseerd. Dit geldt zowel voor verzonden als voor ontvangen privémails. Deze goede praktijk kadert in de bescherming van de privacy van het personeelslid bij toegang tot de mailbox i.k.v. het verzekeren van de continuïteit van de werking of controle.

Elektronische communicatie voor privédoeleinden blijft, indien toegestaan door de werkgever, beperkt en occasioneel, doet geen afbreuk aan de goede werking en veiligheid van het netwerk en de productiviteit van de medewerker of collega’s en vormt geen inbreuk op de van kracht zijnde richtlijnen en wet- en regelgeving.

6.3. Afwezigheidsassistent

Maak gebruik van afwezigheidsboodschappen, zowel voor intern als extern mailverkeer. Je vermeldt hierin wie gecontacteerd kan worden tijdens jouw afwezigheid en wanneer je terug bereikbaar bent Ook bij langdurige afwezigheid worden afspraken gemaakt binnen het CLB.

6.4. Bescherming van vertrouwelijkheid van gegevens

**Check** de bestemmeling vooraleer u mails verstuurt. Zorg ervoor dat mails niet bij de verkeerde personen terecht komen, zeker indien ze vertrouwelijke gegevens bevatten.

Vertrouwelijke gegevens worden niet zomaar via e-mail meegedeeld. Gegevens zoals paswoorden, toegangscodes, persoonlijke gegevens enz. mogen niet via e-mail worden meegedeeld, tenzij op een beveiligde manier. Daarom worden mails steeds geëncrypteerd verstuurd.

6.5. Veilig omgaan met e-mail

Wees alert bij de behandeling van mails. E-mail is geen waterdicht, veilig communicatiemiddel. Het CLB implementeert technische veiligheidsmaatregelen om te vermijden dat schadelijke toepassingen in de mailbox terechtkomen. Het is verboden deze instellingen te deactiveren of de beveiligingssystemen te omzeilen.

Het openen van bijlagen die afkomstig zijn van onbekende, onbetrouwbare personen kan ernstige gevolgen hebben voor het interne netwerk en voor de gegevens die in dit netwerk zijn opgeslagen. Hetzelfde geldt voor het aanklikken van links die zich in een mail bevinden.

Klik niet zomaar een link in een mail aan en wees alert bij het openen van bijlagen. Ga vooraf na wie de verzender is. Zet je leesvenster uit om te voorkomen dat je automatisch virussen binnenhaalt.

Het ingeven van je emailadres op een website of reageren op een mail/forum kan ertoe lijden dat je slachtoffer wordt van spam-mails.

6.6. Beheer van mails

Mails worden bewaard bij de dossiers/ op de plaats waar ze horen. Bewaar ze niet in de persoonlijke mailbox maar zorg dat de informatie gedeeld wordt. Klasseer mails zo snel mogelijk, bij voorkeur onmiddellijk bij ontvangen/verzenden en verwijder ze daarna uit de mailbox. Ken een duidelijke, betekenisvolle bestandsnaam toe aan de mail en bijlagen die je opslaat. Zie Werkinstructie Beheer e-mail.

Mailboxen worden regelmatig opgeruimd waarbij relevante mails opgeslagen worden op de plaats waar ze thuishoren en mails met puur informatieve waarde verwijderd worden uit de mailbox.

Bij uitdiensttreding, veranderen van functie of langdurig verlof wordt de mailbox steeds opgeruimd door het personeelslid vooraleer die gedeactiveerd of afgesloten wordt.

6.7. Meldplicht voor kwetsbaarheden, bedreigingen en incidenten

Bij vermoeden of vaststellen van bedreigingen, kwetsbaarheden en incidenten met mail neem je contact op met uw aanspreekpunt informatieveiligheid (bv. ontvangen van mails die je niet vertrouwt, het aanklikken van corrupte links,…). Op die manier kunnen we zo snel mogelijk remediëren. (zie Procedure Incidentmelding)

6.8. Controle op gebruik van e-mail

De directie van het CLB kan controles uitoefenen op het gebruik van e-mail. Dit kan echter alleen onder bepaalde omstandigheden en in naleving van de wetgeving (o.m. betreffende de bescherming van de persoonlijke levenssfeer). Dit moet opgenomen worden in het arbeidsreglement en/of gedragscode. Misbruik kan gesanctioneerd worden.

7. Bijlage(n)

Werkinstructie Beheer e-mail