Bijlage 4 – Deontologische ICT-code

1 Belangrijk

Deze deontologische ICT-code vormt onlosmakelijk een geheel met de bepalingen met betrekking tot ICT-middelen in het arbeidsreglement.

2 Gedragslijn voor besturen en directeur

Het schoolbestuur en de directeur schikken zich in hun elektronische communicatie met het Ministerie Onderwijs en Vorming naar de gebruiksvoorwaarden zoals vastgelegd in de omzendbrief PERS/2011/2 “Gebruiksvoorwaarden van de elektronische communicatie tussen inrichtende machten en het departement Onderwijs en Vorming – vervanging basisovereenkomst voor elektronische gegevensoverdracht”, van 11 april 2011.

3 Gedragslijn voor de personeelsleden

3.1 Voorbeeldfunctie

Het personeelslid is zich bewust van zijn voorbeeldfunctie ten aanzien van leerlingen en vertegenwoordigt zelf permanent de attitudes die de school inzake het gebruik van ICT-middelen van leerlingen verwacht.

3.2 Algemeen

3.2.1 Het personeelslid verschaft zich geen toegang tot informaticasystemen binnen of buiten de school waartoe het niet geautoriseerd is, zelfs niet indien deze toegang onbelemmerd is of de toegangsbeveiliging op eenvoudige wijze te omzeilen is.

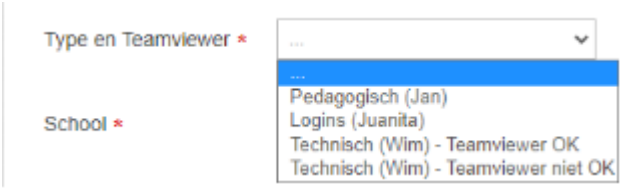
3.2.2 Het personeelslid zal zich geen toegang verschaffen tot bestanden of e-mails van leerlingen of deze raadplegen, zonder de voorafgaande toestemming van de betrokken leerlingen en ouders.

3.2.3 Als u toestemming geeft om via teamviewer geholpen te worden, kan de IT-dienst in de eerstvolgende dagen mogelijk uw computer even overnemen om het probleem van op afstand proberen op te lossen.

Dit is zeker geen verplichting, maar op die manier bent u meestal sneller geholpen.

Als de IT-dienst bij het overnemen merkt dat u de computer op dat moment intensief aan het gebruiken bent om uw bord te bedienen, dan sluiten we de teamviewer sessie en proberen we het opnieuw op een later moment, zodat u er geen hinder van ondervindt.

Wanneer u na het maken van het ticket toch de toestemming wil intrekken is dat geen probleem, u kan het ticket heropenen en de toestemming intrekken.



3.3 Het gebruik van professionele ICT-middelen

3.3.1 Het personeelslid streeft ernaar de professionele ICT-middelen zorgvuldig en correct te gebruiken en ze aan te wenden op de wijze waarvoor ze bestemd zijn. Het personeelslid waakt erover apparatuur niet bloot te stellen aan beschadiging of diefstal, in het bijzonder bij gebruik op verplaatsing.

3.3.2 Het personeelslid vermijdt de professionele ICT-middelen onnodig te belasten, bijvoorbeeld inzake opslagcapaciteit, verwerkingscapaciteit of netwerkverkeer, en vermijdt excessief papierverbruik. Het personeelslid waakt erover overbodig geworden bestanden geregeld te verwijderen of te verplaatsen naar offline gegevensdragers.

3.3.3 Het personeelslid respecteert de aanwezige voorzieningen, bijvoorbeeld inzake energieverbruik, ergonomie en toegangsbeveiliging van de werkpost, inzake de beveiliging van het systeem, het netwerk en de bestanden, inzake de bescherming tegen gegevensverlies, malafide software, ongewenste mail, enz. Het personeelslid zal deze voorzieningen niet hinderen of omzeilen, en zal ze niet uitschakelen zonder voorafgaande toestemming van de bevoegde persoon of de directeur.

3.3.4 Het personeelslid meldt elke disfunctie van de professionele ICT-middelen (zoals o.a. beveiligingsproblemen) en elk redelijk vermoeden van verdachte activiteiten op de computer of het netwerk onmiddellijk aan de bevoegde persoon.

3.3.5 Uitsluitend de bevoegde persoon is bevoegd om software te installeren of te de-installeren op de computers van de school, om andere apparatuur dan deze van de school op een computer of op het netwerk aan te sluiten, of om apparatuur te ontkoppelen. Deze bevoegde persoon mag software of apparatuur verwijderen die zonder toestemming geïnstalleerd of aangesloten is.

3.3.6 In afwijking van punt 3.3.5 mag het personeelslid externe gegevensdragers (bijvoorbeeld externe harde schijven, USB-sticks) op de computers aansluiten. Het personeelslid waakt erover deze externe gegevensdragers vrij te houden van malafide software en tegen misbruik of vervreemding te beschermen.

3.3.7 In afwijking van punt 3.3.5 mogen leraren, en de leerlingen die onder hun toezicht staan, werkzaamheden verrichten die voor de realisatie van leerplannen ICT of informatica nodig geacht worden. Ze waken erover hierdoor de operationaliteit van het netwerk niet te schaden en de apparatuur en de software steeds in gebruiksklare toestand achter te laten.

3.3.8 Het personeelslid kan aan de bevoegde persoon voorstellen bepaalde software te installeren of bepaalde apparaten aan te sluiten, bijvoorbeeld omdat de aanwezigheid ervan wenselijk of noodzakelijk is voor de realisatie van een leerplan. Indien deze bevoegde

persoon met voormeld voorstel niet instemt, kan het personeelslid zijn vraag voorleggen aan de directeur, die beslist.

3.3.9 Het personeelslid verwijdert geen documenten of bestanden van een andere persoon, tenzij met uitdrukkelijke toestemming van deze persoon. Als de toestemming niet aan deze persoon gevraagd kan worden, verwijdert het personeelslid de documenten of bestanden uitsluitend met de toestemming van de directeur.

3.4 Het gebruik van netwerken op school

3.4.1 Het personeelslid ontvangt een individuele gebruikersnaam (inlogcode) waarmee het toegang krijgt tot het schoolnetwerk, het intranet en/of de elektronische leeromgeving (elo), zowel op school als thuis. De toegangsrechten kunnen verschillen van personeelslid tot personeelslid.

3.4.2 Het personeelslid waakt erover zijn wachtwoord (password) strikt geheim te houden, deelt het aan niemand mee en bewaart het niet in papieren versie. Het personeelslid wijzigt zijn wachtwoord als het vermoeden bestaat dat een derde over zijn gebruikersnaam en wachtwoord beschikt of als de bevoegde persoon hem dat vraagt.

3.4.3 Het personeelslid geeft derden geen toegang tot het schoolnetwerk, het intranet of de elektronische leeromgeving via zijn gebruikersnaam en wachtwoord, zelfs niet voor korte duur. Indien het personeelslid ingelogd is, verlaat het zijn werkpost niet zonder uit te loggen of de toegang tot de werkpost af te sluiten. Handelingen die op het schoolnetwerk, het intranet of de elektronische leeromgeving gesteld worden, worden in principe vermoed verricht te zijn door het personeelslid wiens gebruikersnaam en wachtwoord daartoe gebruikt zijn.

3.5 Het gebruik van e-mail

3.5.1 Het personeelslid ontvangt van de school een individueel e-mailadres voor professioneel gebruik. Dit e-mailadres en het bijbehorend wachtwoord zijn aan dezelfde gedragslijn onderworpen als de gebruikersnaam en het wachtwoord voor de toegang tot het schoolnetwerk (zie punt 3.4).

3.5.2 Door de ontvangst van dit professioneel e-mailadres erkent het personeelslid e-mail als één van de mogelijke communicatievormen tussen hem, het leidinggevend personeel en het schoolbestuur.

3.5.3 Het personeelslid gebruikt zijn professioneel e-mailadres enkele voor professionele doeleinden.

3.5.4 Het personeelslid controleert geregeld de inhoud van zijn mailbox en volgt zijn e-mail binnen een redelijke termijn op.

3.5.5 Elk personeelslid stelt bij geplande afwezigheid een automatisch antwoord ('out of office reply') in waarin zijn afwezigheid wordt bevestigd. In geval van onvoorziene afwezigheid wordt het automatisch antwoord ingesteld door de bevoegde persoon.

3.5.6 Het personeelslid is steeds alert voor inkomende mail van verdachte, aanstootgevende of frauduleuze aard. Het personeelslid opent geen mails of aangehechte documenten van kennelijk verdachte herkomst of aard. Het personeelslid verwijdert alle ongewenste mails definitief. Het personeelslid lanceert zelf geen kettingbrieven, ongewenste reclame (spam) of andere ongewenste berichten, en waakt erover dergelijke berichten niet te beantwoorden of door te sturen.

3.5.7 Het personeelslid meldt pogingen tot fraude of tot het achterhalen van informatie die niet publiek is aan de bevoegde persoon of aan de directeur.

3.5.8 Het personeelslid neemt in zijn elektronische communicatie nooit de identiteit van een andere persoon aan.

3.5.9 Het personeelslid hanteert verzorgd taalgebruik in zijn mails.

3.5.10 Telkens de samenwerking of de informatieverstrekking dit vereist, brengt het personeelslid de directeur en/of andere personeelsleden op de hoogte van de inhoud van e-mails met een professioneel karakter.

3.5.11 E-mails met een privékarakter kunnen enkel met uitdrukkelijke toestemming van het personeelslid en andere betrokkenen door directeur en/of andere personeelsleden ingezien worden.

3.6 Het gebruik van het internet

3.6.1 Het personeelslid gebruikt de internetaansluiting van de school hoofdzakelijk voor professionele doeleinden.

3.6.2 Indien de internetaansluiting van de school ook voor persoonlijke doeleinden gebruikt wordt, gebeurt dit met mate, zonder de transmissiesnelheid of het downloadvolume buitensporig te belasten en zonder de wettelijke bepalingen en de bepalingen van punt 3.2 te schenden. Downloadvolumes voor persoonlijke doeleinden kunnen beperkt worden.

3.6.3 Het personeelslid plaatst geen webpagina's voor persoonlijk gebruik of voor commerciële doeleinden op servers die eigendom zijn van of die gebruikt, gehuurd of geleased worden door de school.

3.6.4 De bevoegde persoon kan in opdracht van de directeur de toegang tot sommige websites voor leerlingen en/of personeelsleden onmogelijk maken.

3.6.5 Indien het personeelslid voor professionele doeleinden geheime toegangscodes ontvangt voor websites van derden, dan zijn deze codes en het bijbehorend wachtwoord

aan dezelfde gedragslijn onderworpen als de gebruikersnaam en het wachtwoord voor de toegang tot het schoolnetwerk (zie punt 3.4).

4 Bevoegde personen

De bevoegde personen (naast de directeurs) zijn:

Wim Verhaeghe
Kris Vandenberghe