# ICT Beveiliging binnen de school
# The DO's en DON'Ts

Gezamenlijk zijn we verantwoordelijk voor onze beveiliging. Volg de tips in dit document en het zal helpen om jezelf, je collega's en onze school veilig te houden. Veiligheid geeft ons de vrijheid om te doen waar we goed in zijn. Het is simpel, maar toch essentieel voor ons bedrijf. Zorg ervoor dat je familie en vrienden weten hoe ze veilig moeten werken, zodat ook zij veilig zijn op het internet.

**1. Laat je niet misleiden door het weggeven van vertrouwelijke informatie**

Reageer nooit op e-mails of telefoontjes waarbij er om belangrijke bedrijfsinformatie gevraagd wordt, zoals informatie over medewerkers, financiële resultaten en bedrijfsgeheimen. Het is makkelijk voor een onbevoegd persoon om ons te bellen en zich voor te doen als een medewerker of een partner. Blijf altijd waakzaam om dit soort situaties te voorkomen. Mocht je toch verdachte telefoontjes of mailtjes tegenkomen, geef het altijd aan bij onze ICT-verantwoordelijken. Zorg ook dat je persoonlijke informatie goed beschermt.

**2. Gebruik nooit een onbeveiligde computer**

Wanneer je gevoelige informatie op een onbeveiligde computer opent, is er een mogelijkheid dat onbevoegde personen de informatie ook kunnen zien. Probeer dit te voorkomen. Zorg dat je de laatste (goedgekeurde) security patches tot je beschikking hebt en dat je antivirus en firewall altijd geüpdatet zijn. Probeer daarnaast altijd in de gebruikersmodus te werken in plaats van de beheerdersmodus. De ICT-afdeling zorgt hiervoor op school.

**3. Laat nooit belangrijke informatie achter in je kantoor of op je werkplek**

Zorg ervoor dat je geen uitgeprinte, belangrijke informatie op je bureau hebt liggen. Belangrijke informatie dien je in een gesloten lade te bewaren of te versnipperen. Houd je bureau netjes en berg belangrijke informatie op. Op deze manier ziet je kantoor er netjes uit en voorkom je het risico dat belangrijke informatie uitlekt.

**4. Vergrendel je computer en telefoon als je er geen gebruik van maakt**

Zorg dat je computer en telefoon te allen tijde vergrendeld zijn als je er geen gebruik van maakt. Je werkt aan belangrijke documenten, dus is het van belang dat deze documenten beveiligd zijn en dat niemand erbij kan. Het vergrendelen van je computer en telefoon zorgt ervoor dat nieuwsgierige mensen niet kunnen meekijken.

**5. Blijf alert en rapporteer verdachte activiteiten**

Verdachte activiteiten op het internet moet je altijd rapporteren bij onze ICT-verantwoordelijken. Een deel van het werk van onze ICT-afdeling  is om cyberaanvallen tegen te gaan en ervoor te zorgen dat er geen documenten zoek raken of gestolen worden. Al onze functies zijn afhankelijk van het beveiligen van onze informatie. In het geval dat er iets fout gaat, is het van belang dat dit aangegeven wordt. Hoe sneller onze ICT-afdeling ervan weet, hoe sneller het probleem opgelost kan worden.



ICT-Afdeling Segbroek College | ict@segbroek.nl | Tel. 293

# ICT Beveiliging binnen de school
# The DO's en DON'Ts

**6. Bescherm belangrijke informatie en apparaten door middel van een wachtwoord.**

Je dient er altijd voor te zorgen dat gevoelige informatie op je computer, USB-stick of smartphone beveiligd is met een wachtwoord. Je smartphone, USB-stick of laptop verliezen kan altijd gebeuren. Het met een wachtwoord beveiligen van deze apparaten maakt het ongelooflijk moeilijk om in te breken en documenten te stelen.

**7. Gebruik altijd moeilijk te raden wachtwoorden**

Gebruik geen makkelijke wachtwoorden zoals "kat" of een makkelijke cijfercombinatie zoals "12345". Het is beter om een ingewikkeld wachtwoord*) te hebben met hoofdletters, nummers en interpunctie. Probeer verschillende wachtwoorden voor verschillende websites te hanteren zodat als er één gehackt wordt, de anderen nog goed beveiligd zijn.

**) $e7enal1ig@t0r5inmyb^th (seven alligators in my bath)*

**8. Wees voorzichtig met verdachte e-mails of links**

Laat je nieuwsgierigheid je niet fataal worden. Verwijder te allen tijde verdachte e-mails of links. Zelfs het openen of het bekijken van deze e-mails en links kan vervelende gevolgen hebben zonder dat je het door hebt. Onthoud: als iets te mooi lijkt om waar te zijn, is dat het waarschijnlijk ook.

**9. Plug nooit persoonlijke apparaten in de apparaten van school zonder toestemming van de ICT-verantwoordelijke**

Plug nooit persoonlijke apparaten zoals een USB-stick of je smartphone in een computer zonder toestemming van de ICT-verantwoordelijke. Deze kunnen worden aangetast op het moment dat je hem aansluit op de computer. Bespreek het eerst met de ICT-afdeling voordat je je persoonlijke apparaat aansluit op je werk.

**10. Installeer nooit onbevoegde programma's op je werkcomputer**

Kwaadaardige programma's lijken er vaak betrouwbaar uit te zien, zoals games, apps en zelfs antivirussoftware. Ze zijn bedoeld om je in de maling te nemen en het zorgt voor virussen op je computer of netwerk. Als je een applicatie tegenkomt die je wilt gebruiken, neem eerst contact op met de ICT-afdeling voordat je de applicatie installeert.

**<u>Voortdurende inspanning</u>**

Zolang computers bestaan zullen de bedreigingen hiervan ook blijven bestaan. Deze top 10-lijst zal naarmate de tijd vordert steeds aangepast moeten worden, omdat er altijd nieuwe bedreigingen ontstaan. Houd de updates van dit handboek in de gaten, zodat jezelf en onze school niet in gevaar zullen komen.



ICT-Afdeling Segbroek College | ict@segbroek.nl | Tel. 293