Do's and don'ts voor studenten

Versie 1

yonder

Yonder heeft een ICT-Gedragscode en een Gedragscode sociale media voor studenten. Dit is een uitgebreid document en we kunnen ons voorstellen dat je je afvraagt wat dat nu voor jou in de praktijk betekent. Daarom hebben we deze do's en don'ts opgesteld. Neem ze eens goed door. De volledige ICT-Gedragscode en Gedragscode sociale media vind je hier.

Heb je nog andere vragen? Mail dan naar privacy@yonder.nl .

1. Omgaan met accountgegevens

Do

- Ga vertrouwelijk om met je account-gegevens van school. Ze zijn strikt persoonlijk.
- Voorkom dat iemand meeleest bij het invullen van je wachtwoord en je schoolaccount daarna kan misbruiken.

Don't

- Geef nooit je accountgegevens aan een ander. Je schoolaccount is persoonlijk net zoals je pincode bijvoorbeeld. Je bent verantwoordelijk voor wat er mee gedaan wordt.
- Leen je schoolaccount ook niet uit.

2. Wachtwoord

Do

- Kies een moeilijk, niet vanzelfsprekend wachtwoord of zelfs een wachtzin*.
- Verander je wachtwoord bij het eerste gebruik en daarna regelmatig. Doe dit meteen als je denkt dat iemand je wachtwoord heeft meegelezen of als je schoolaccount is 'gehackt'.

Don't

- Gebruik je accountnaam niet als wachtwoord.
- Gebruik geen voor de hand liggende gegevens over jezelf zoals naam en leeftijd of combinaties hiervan (bijvoorbeeld Janneke17).
- Gebruik voor jouw schoolaccount geen wachtwoorden die je ook voor andere sites gebruikt. Dit voorkomt dat een hacker van een andere site gemakkelijk bij jouw schoolaccount kan.

* Een 'sterk' wachtwoord maak je door de eerste letters van een makkelijk te onthouden zin te gebruiken en één of twee letters te veranderen in tekens. 'Mijn tweede Ipad is zwart' wordt M2eiPadiZ.

3. Datalekken

Do

- Meld beveiligingsincidenten, phishing mails die je op je schoolaccount ontvangt of 'hacking' van je schoolaccount altijd bij de Servicedesk of de schooldirect.
  Meld dit meteen en wacht hier niet mee.

Don't

- Gebruik geen niet-versleutelde usb-sticks en laptops om datalekken te voorkomen.
- Leen geen externe opslagmedia uit aan andere studenten.

4. Bestanden bewaren en bewerken

Do	Don’t
Sla belangrijke bestanden op en/of bewerk deze in de hiervoor ingerichte applicatie EduArte of op de SharePoint site of OneDrive.	Sla belangrijke gegevens niet op het bureaublad van de lokale computer op. Bij een crash ben je deze onherroepelijk kwijt.
Maak je gebruik van externe opslagmedia, bijvoorbeeld een usb-stick, externe harde schijf of een mobiele telefoon? Dan dient deze versleuteld te zijn met een code of swipe.	De ontgrendelcode van bijvoorbeeld een mobile device mag geen “0000” of andere gemakkelijke code zijn.

5. Computergebruik

Do	Don’t
Lock je computer, ook als je tijdelijk je studieplek verlaat.	Installeer of activeer geen illegale of overbodige programmatuur.
Installeer met regelmaat updates van je besturingssysteem.	Doe niet aan hacking, spoofing enz. Dergelijk misbruik is een misdrijf. Dit is computercriminaliteit. Wij doen aangifte.
Voorkom verspreiding van computervirussen. Wees voorzichtig bij het openen van bijlagen, linkjes en programma's op internet. Installeer ook op je thuis-computer of laptop een antivirusprogramma en houd dit actueel.	Sluit geen netwerkapparatuur (zoals routers en switches) op het schoolnetwerk aan.
Beperkt privégebruik van het netwerk is toegestaan, maar zodanig dat het netwerk van de school hiervan geen nadeel heeft.	Doe niet mee aan 'kettingmail' (forwarden).
	Download geen films, software of foto's voor persoonlijk gebruik.
	Gebruik je computers van school niet voor commerciële doeleinden.
	Je docent kan je nooit verplichten tot het gebruik van bepaalde gratis applicaties.

6. Smartphones

Do	Don't
Beveilig je smartphone met een code of swipe om deze te ontgrendelen.	Maak nooit beeld- of geluidsopnamen zonder toestemming van de mede-studenten en docenten. Vraag eerst altijd toestemming.
Gebruik WhatsApp en andere social media netjes.	Laat je smartphone niet onbeheerd achter en leen deze niet uit om misbruik te voorkomen.

7. Social Media

Do	Don't
Gebruik je sociale media platforms (zoals Facebook, YouTube, Instagram, Twitter of SnapChat) zorg dan dat je je netjes gedraagt.	Reageer niet op kritische commentaren. Iedereen heeft recht op zijn/haar mening.
Gebruik je schoolaccount op dezelfde manier als je privé accounts.	Gebruik geen dreigende, (seksueel) intimiderende taal in chats of op sociale media.
Als je een negatief of kwetsend bericht over de school of over docenten en medestudenten op social media ziet, meldt dit dan bij je mentor (SLB-er) of de schooldirecteur.	Plaats geen foto's van docenten en medestudenten op je privé account (zoals Instagram of Snapchat).
Onthoud dat online dezelfde sociale omgangsvormen en fatsoensnormen gelden als offline.	Stuur geen vriendschapsverzoeken via sociale media platforms naar docenten. Communiceer met docenten via de daarvoor aangewezen formele kanalen (zoals Teams, EduArte, schoolmail e.d.).

8. Wettelijke bepalingen

Do

- Houd je aan de wet!
- Behandel anderen zoals je zelf behandeld wilt worden.
- Houd je aan de reguliere fatsoensnormen.
- Meld overtredingen bij je mentor of de schooldirecteur.

Don’t

- Zet geen op school gemaakt geluid- of beeldmateriaal op internet.
- Sla geen auteursrechtelijk beschermde bestanden (boeken, films, muziek) op.
- Gebruik geen dreigende, (seksueel) intimiderende taal in e-mail-, chat- of sociale media.
- Ga niet naar internetsites met pornografisch, racistisch, of anderszins discriminerend materiaal.
- Sla geen (kinder-)pornografische afbeeldingen op.
- Publiceer geen vertrouwelijke informatie over jezelf, medestudenten of de school op bijvoorbeeld sociale media.