## Checklist Digitale Hygiëne – Veilig gedrag in onderwijs en AI

Digitale hygiëne gaat over bewust en veilig omgaan met digitale middelen. Deze checklist helpt iedereen binnen de organisatie – van studenten tot directie – om verantwoordelijkheid te nemen voor digitaal veilig gedrag. AI en technologie maken ons werk efficiënter, maar alleen als we zorgvuldig blijven handelen.

### 1. Studenten / Leerlingen

- • Gebruik alleen schoolaccounts voor opdrachten en communicatie.
- • Deel geen wachtwoorden, persoonlijke gegevens of foto's via publieke AI-tools.
- • Controleer of de AI-tool die je gebruikt door school is goedgekeurd.
- • Vraag altijd toestemming als je werk of data van anderen gebruikt.
- • Reflecteer in opdrachten eerlijk op je eigen AI-gebruik.

### 2. Docenten

- • Gebruik AI-tools alleen binnen afgesproken kaders en vermeld dit in lesmateriaal.
- • Begeleid studenten actief in verantwoord gebruik van AI en digitale bronnen.
- • Bewaar leerlingwerk en feedback op beveiligde schoolservers, niet lokaal of in publieke clouds.
- • Controleer regelmatig of accounts en wachtwoorden veilig zijn ingesteld.
- • Meld onveilige situaties direct bij ICT-beheer of de privacy officer.

### 3. Ondersteunende diensten (administratie, facilitair, communicatie)

- • Verwerk geen persoonsgegevens in AI-tools of onbeveiligde platforms.
- • Gebruik officiële communicatiekanalen (Teams, Outlook) voor schoolzaken.
- • Sluit je computer altijd af of vergrendel bij afwezigheid.
- • Houd documenten met privacygevoelige informatie offline of in beveiligde mappen.

### 4. Managers / Teamleiders

- • Stimuleer veilig digitaal gedrag in je team en geef zelf het goede voorbeeld.
- • Bespreek regelmatig digitale veiligheid in teamvergaderingen.
- • Toets of gebruikte software en AI-tools voldoen aan de AVG.
- • Zorg voor duidelijke werkafspraken en meldprocedures bij incidenten.
- • Ondersteun collega's bij twijfel over veilig gebruik van data of AI.

### 5. Directeuren / Bestuurders

- • Stel jaarlijks prioriteiten vast op het gebied van digitale veiligheid en AI.
- • Zorg dat beleid, middelen en scholing structureel geborgd zijn.
- • Stimuleer openheid over fouten of incidenten – leren van fouten is veiliger dan ze verbergen.
- • Houd toezicht op naleving van het veiligheidsprotocol en privacybeleid.

## 6. ICT-beheer

- • Controleer regelmatig logbestanden en toegangsrechten van gebruikers.
- • Houd systemen, servers en AI-tools up-to-date met beveiligingsupdates.
- • Informeer gebruikers actief over risico's van nieuwe technologieën.
- • Documenteer incidenten en deel bevindingen met het management.
- • Evalueer jaarlijks het beleid rond digitale veiligheid en AI-gebruik.

## Digitale hygiëne is teamsport

Digitale veiligheid ontstaat door samenwerking. Iedereen – van student tot bestuurder – speelt een rol in het beschermen van gegevens, systemen en reputatie. Gebruik deze checklist jaarlijks als onderdeel van het veiligheids- of kwaliteitsbeleid.

---

Meer handvatten: boek *AI voor de klas* – www.aivoordeklas.nl