Voorbeeld Veiligheidsprotocol – Digitale Veiligheid & AI

Dit document biedt een voorbeeld van een veiligheidsprotocol voor onderwijsinstellingen. Het beschrijft basisafspraken en verantwoordelijkheden rond digitale veiligheid, inclusief het gebruik van AI-tools. Het protocol kan worden aangepast aan de lokale context van de school.

1. Doel en reikwijdte

Het doel van dit protocol is om de digitale veiligheid binnen de organisatie te waarborgen en bewust gedrag te stimuleren bij medewerkers, studenten en partners. Het protocol geldt voor alle digitale systemen, apparaten, netwerken en AI-toepassingen die binnen de school worden gebruikt.

2. Basisprincipes van digitale veiligheid

De organisatie hanteert de volgende uitgangspunten:

- • Veiligheid vóór gemak – bewust kiezen voor betrouwbare, getoetste technologie.
- • Privacy en integriteit – persoonsgegevens worden beschermd en alleen gedeeld waar nodig.
- • Transparantie – gebruikers weten wat er met hun data gebeurt.
- • Eigen verantwoordelijkheid – iedere gebruiker draagt bij aan digitale veiligheid.

3. AI-specifieke richtlijnen

Om veilig en verantwoord gebruik van AI binnen de organisatie te waarborgen, gelden de volgende richtlijnen:

- • Gebruik geen publieke AI-tools voor vertrouwelijke of privacygevoelige informatie.
- • Controleer altijd of de gebruikte AI-tool voldoet aan de AVG en is goedgekeurd door ICT-beheer.
- • Vermeld bij producten of rapportages wanneer AI is ingezet.
- • Gebruik AI alleen als hulpmiddel ter ondersteuning van leren, lesgeven of organiseren – niet ter vervanging van menselijke beoordeling.
- • Meld onbedoelde data-invoer of incidenten direct bij ICT-beheer.

4. Rollen en verantwoordelijkheden

Per rol gelden de volgende verantwoordelijkheden:

- Docenten:
    - – Geven het goede voorbeeld in veilig AI- en internetgebruik.
    - – Begeleiden studenten in verantwoord gebruik van digitale middelen.
- Studenten:

- – Gebruiken schoolaccounts en systemen uitsluitend voor onderwijsdoeleinden.
- – Delen geen vertrouwelijke informatie met AI-tools of externe platforms.

- ICT-beheer:
  - – Beoordeelt en autoriseert AI-tools en software op veiligheid en privacy.
  - – Houdt toezicht op beveiliging van netwerken, servers en gebruikersaccounts.

- Management/Directie:
  - – Zorgt voor beleid, middelen en scholing op het gebied van digitale veiligheid.
  - – Stimuleert een cultuur waarin veilig gedrag normaal is en incidenten gemeld kunnen worden.

5. Incidenten en meldplicht

Bij een vermoeden van een beveiligingsincident of datalek gelden de volgende stappen:

1. 1. Meld het incident direct bij ICT-beheer of de privacy officer.
2. 2. Beschrijf kort wat er is gebeurd, welke gegevens mogelijk betrokken zijn en wie toegang had.
3. 3. ICT-beheer onderzoekt het incident en rapporteert binnen 24 uur aan het management.
4. 4. Indien nodig wordt het incident gemeld bij de Autoriteit Persoonsgegevens.

6. Evaluatie en onderhoud

Het veiligheidsprotocol wordt jaarlijks geëvalueerd door ICT-beheer en het managementteam. Nieuwe risico's (zoals ontwikkelingen binnen AI) worden meegenomen in de actualisatie. Medewerkers en studenten worden actief geïnformeerd over wijzigingen.
