Regels informatiebeveiliging
'Iedereen een Meester'

- Medewerkers en vrijwilligers dienen zorg te dragen voor een clean desk.
- Medewerkers en vrijwilligers dienen alle door de organisatie, zowel Iedereen een Meester als de school waar iemand werkzaamheden verricht, ter beschikking gestelde ICT-middelen te voorzien van deugdelijke wachtwoorden en toegangscontroles.
- Medewerkers en vrijwilligers mogen hun wachtwoorden niet delen met derden; deze wachtwoorden zijn uitsluitend voor persoonlijk gebruik.
- Medewerkers en vrijwilligers dienen hun wachtwoorden vast te leggen in een fysieke of digitale kluis; wachtwoorden mogen dus niet opgeschreven en/of vastgelegd worden op een voor derden toegankelijke plek.
- Medewerkers en vrijwilligers dienen hun wachtwoorden onmiddellijk te wijzigen indien het vermoeden bestaat dat dit wachtwoord bekend is geworden bij een derde.
- Medewerkers en vrijwilligers dienen misbruik van wachtwoorden als beveiligingsincident te melden bij de vertrouwenspersoon van Iedereen een Meester.
- Wachtwoorden mogen niet overeenkomen met wachtwoorden die gehanteerd worden voor privé doeleinden.
- Medewerkers en vrijwilligers dienen ervoor zorg te dragen dat derden niet ongeoorloofd van hun beeldscherm kunnen meelezen.
- Medewerkers en vrijwilligers dienen hun computer te vergrendelen bij het verlaten van de werkplek.
- Medewerkers en vrijwilligers dienen privacygevoelige gegevens uitsluitend op te slaan in officiële bedrijfssystemen; het gebruik van niet beveiligde externe informatiedragers zoals USB- sticks is daarvoor niet toegestaan.
- Medewerkers en vrijwilligers dienen uitsluitend up-to-date software te gebruiken.

- Medewerkers en vrijwilligers dienen uitsluitend in te loggen op een beveiligd (openbaar) wifi-netwerk.

- Medewerkers en vrijwilligers mogen privacygevoelige gegevens uitsluitend uitwisselen op een veilige, versleutelde manier.

- Medewerkers en vrijwilligers dienen privacygevoelige informatie die geprint wordt direct van de printer te halen.

- Medewerkers en vrijwilligers dienen hun kantoor en/of kasten met daarin privacygevoelige informatie bij vertrek af te sluiten.

- Medewerkers en vrijwilligers dienen direct melding te maken van een mogelijk risico dat derden ongeoorloofd toegang hebben gekregen dan wel kunnen krijgen tot privacygevoelige informatie (door bijvoorbeeld verlies en/of diefstal van een laptop, mobiele telefoon of papieren) bij de vertrouwenspersoon van Iedereen een Meester.

Bovenstaande regels zijn vastgelegd in het kader van de AVG. Mochten bovenstaande regels in de toekomst wijzigingen dan worden alle betrokkenen daarover geïnformeerd.

Vaststelling regels informatiebeveiliging

Deze regels omtrent informatiebeveiliging zijn vastgesteld op 20 september 2021 te Den Haag door het bestuur van de Stichting Iedereen een Meester.

Met ingang van 20 september 2021 heeft het bestuur Margôt Hart benoemd tot vertrouwenspersoon van IeM. De vertrouwenspersoon is bereikbaar via info@iedereeneenmeester.nl.