Procedure voor scholen bij het vermoeden van een beveiligingsincident.

Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie-verwerkende systemen in gevaar is of kan komen.
Enkele voorbeelden van beveilingingsincidenten zijn besmettingen met virussen en/of malware, pogingen om ongeautoriseerd toegang te krijgen tot informatie of systemen (hacken), verlies van usb-stick met gevoelige informatie, diefstal van data of hardware.

Procedure Cadans primair:

1. Bij vermoeden van een beveiligingsincident dient medewerker (mits dit mogelijk is) een foto te maken van het incident en vervolgens onmiddellijk PC/laptop af te sluiten. Medewerker neemt zelf (of via directeur van school) direct contact op met support van Drie-O telefoon: 0413-490620.

   (Buiten kantoortijden kan de directeur van Drie-O ,Mark Wijgergangs gebeld worden op 06-53778665 of men kan een WhatsApp sturen).

   Interne procedure Drie-O:
   - Hoofdsysteembeheerder en directeur van Drie-O worden direct ingelicht over het incident.
   - Drie-O zal direct het wachtwoord van de medewerker wijzigen.
   - Vervolgens zullen zij de bovenschoolse ict-er inlichten.

2. Medewerker dient z.s.m. de volgende informatie aan te leveren aan Drie-O per mail of telefoon:
   Naam van de school
   Naam medewerker, gebruikers account en telefoonnummer waarop de medewerker te bereiken is.
   Tijdstip van het incident
   Omschrijving van het incident
   Eventueel printscreens of foto's van het incident

3. Drie-O zal regelmatig de voortgang van het onderzoek doorgeven aan bovenschools ict-er

4. Wanneer de schade door het beveiligingsincident is opgelost en het ICT systeem weer wordt vrijgegeven zal Drie-O de bovenschools ict-er daarover informeren.

5. In overleg met de bovenschools ict-er en bestuurder van de stichting dient bepaald te worden of er melding moet worden gedaan van het beveiligingsincident richting de Autoriteit Persoonsgegevens.

6. Evaluatie
   Binnen een week na het oplossen van het beveiligingsincident wordt er een overleg gepland om het e.e.a. te evalueren en verbetermaatregelen door te voeren.

7. Stichting dient zelf te bepalen of zij het nodig acht e.e.a. naar de buitenwereld te communiceren (b.v. ouders).
   Communicatie binnen de stichting is de verantwoordelijkheid van de stichting zelf.

** Bij afwezigheid van de bovenschools ict-er zal direct contact opgenomen worden met Michelle Bosmans*