

Model Responsible Disclosure voor leerlingen

Voorbeelddocument

Versie: Oktober 2024



**Let op: verwijder deze pagina voor gebruik**

**Over dit voorbeelddocument**

**Dit voorbeelddocument helpt je met het maken van een eigen model Responsible Disclosure voor leerlingen. Elke school en elk schoolbestuur is anders. Pas het document daarom aan aan jouw eigen situatie.**

**Aanpassen van dit voorbeelddocument**

Let bij het aanpassen van het document op het volgende:

* Bij hoofdstukken en paragrafen zijn soms toelichtingen geplaatst. Verwijder deze voordat je het model definitief maakt.
* Dit model gaat ervan uit dat taken, rollen en functies die nodig zijn om het proces uit te voeren bij de juiste personen belegd zijn. Is dit niet zo? Ga dan eerst naar fase 1 van het Groeipad.
* Geel gearceerde teksten moet je vervangen door eigen tekst.

**Totstandkoming**

Dit voorbeelddocument is samengesteld door Kennisnet. Binnen het programma Digitaal Veilig Onderwijs bundelen het ministerie van OCW, Kennisnet, SIVON, de PO-Raad en de VO-raad hun krachten voor een onderwijssector waarin iedere leerling digitaal veilig kan leren en medewerkers digitaal veilig kunnen werken.

**Sommige rechten voorbehouden**

Hoewel aan dit document de uiterste zorg is besteed, aanvaardt Kennisnet geen aansprakelijkheid voor eventuele fouten of onvolkomenheden. Ook aanvaardt Kennisnet geen enkele aansprakelijkheid voor schade van welke aard dan ook, ontstaan uit het (onjuiste) gebruik van dit document.



Dit template is opgesteld door Kennisnet en verschijnt onder de licentie [*Creative Commons Naamsvermelding 4.0 Nederland*](https://creativecommons.org/licenses/by/4.0/legalcode.nl).

**Vragen?**

Heb je vragen over dit voorbeelddocument? Kijk voor meer informatie op [*normenkaderibp.kennisnet.nl/groeipad*](file:///Users/jhgerrits/Documents/1.%20Kennisnet%20voorbeeldocumenten/normenkaderibp.kennisnet.nl/groeipad)of stuur een mail naar *ibp@kennisnet.nl**.*

**Documentgeschiedenis**

***Toelichting***

* *Geef hier aan wie het document vaststelt. Dat kan bijvoorbeeld de proceseigenaar zijn, maar ook het bestuur.*
* *Geef aan of het document openbaar, vertrouwelijk of geheim is en wie het in die gevallen mogen zien.*

**Revisies**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Auteur** | **Review** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Vaststelling**

|  |  |  |  |
| --- | --- | --- | --- |
| **Naam** | **Functie** | **Versie** | **Datum** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Documentclassificatie**

|  |  |
| --- | --- |
| **Classificatie** | **Beschrijving** |
| Openbaar | Dit document mag zonder beperkingen worden gedeeld |
| Vertrouwelijk | Dit document mag worden gedeeld met medewerkers van <naam schoolbestuur en eventuele andere organisaties> |
| Geheim | Dit document is exclusief bestemd voor de volgende personen: <bijv. leden MT>. |

# Model Responsible Disclosure voor leerlingen

***Toelichting***

*Let op: Alle gele onderdelen invullen op basis van de gegevens van de eigen organisatie.*

Bij <schoolbestuur> vinden wij de veiligheid van onze informatiesystemen (internet en bijbehorende hardware en software) erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek (kwetsbaarheid) is. Heb jij een zwakke plek in één van onze systemen hebt gevonden? Dan horen wij dit graag, zodat we zo snel mogelijk maatregelen kunnen treffen. Wij willen graag met jou samenwerken om de leerlingen, medewerkers en onze systemen beter te kunnen beschermen.

Wij vragen jou:

* Je bevindingen te mailen naar <security@<schoolbestuur>.nl of deze door te geven aan je <mentor>. Jouw <mentor> zal je vervolgens in contact brengen met onze <security officer>.
* De kwetsbaarheid niet te misbruiken, geen data te downloaden of informatie van andere leerlingen, docenten of medewerkers in te kijken, te verwijderen of aan te passen.
* De kwetsbaarheid niet met anderen te delen totdat deze is verholpen en alle informatie die verkregen is via het lek direct na het verhelpen van het lek te wissen.
* Geen gebruik te maken van aanvallen op de beveiliging van de school, zoals spam of DDoS-aanvallen.
* De school voldoende informatie te geven om het probleem te kunnen vinden zodat wij het zo snel mogelijk kunnen verhelpen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij meer ingewikkelde kwetsbaarheden kan extra informatie nodig zijn.

Wij beloven dat:

* Je binnen (optioneel: 3 (werk)dagen) van ons te horen krijgt hoe we de kwetsbaarheid gaan oppakken en wanneer wij hiervoor een oplossing verwachten te hebben.
* Als je de kwetsbaarheid netjes gemeld hebt en via de bovenstaande stappen gehandeld hebt, zullen wij geen melding maken bij de politie of juridische stappen ondernemen\*.
* Wij zullen jouw melding vertrouwelijk behandelen en jouw persoonlijke gegevens niet zonder jouw toestemming met anderen delen worden tenzij dit wettelijke verplicht is.
* (Optioneel) Als je de kwetsbaarheid gemeld hebt volgens bovenstaande stappen, ontvang je van ons een passende beloning.
* Wij zullen je op de hoogte houden van de voortgang van het verhelpen van de kwetsbaarheid.

\* **Let op**: ons beleid voor responsible disclosure is geen uitnodiging om ons netwerk uitgebreid te scannen om zwakke plekken te ontdekken. Het is onze eigen verantwoordelijkheid om ons netwerk te monitoren. Er bestaat een kans dat je tijdens jouw ‘zoektocht’ handelingen uitvoert die strafbaar zijn. Het feit dat <schoolbestuur> geen aangifte tegen je zal doen sluit niet uit dat er een strafrechtelijk onderzoek naar jouw handelen gehouden kan worden dan wel dat je strafrechtelijk kunt worden veroordeeld.

Cc/by/3.0 NL

Geschreven door Floor Terra (responsibledisclosure.nl), bewerkt door Kennisnet en <schoolbestuur>.