Responsible Disclosure Policy

The Future Foundation (Stichting “The Future”)
Last updated: February 15, 2018

We (The Future Foundation) take privacy and security seriously. Still there is a possibility that our website or e-mail services are vulnerable to bugs, hacks or data breaches.
We very much appreciate it if you notify us of these vulnerabilities in the form of a “Responsible Disclosure”.

Contact information:
For responsible disclosure, you can use our regular contact information.

	Stichting The Future
Street:	Govert Flinckstraat
housenumber:	16
postal code:	2923AC
city:	Krimpen aan den Ijssel
telephone:	+31 180 552091
e-mail:	info@stichtingthefuture.nl

Please state clearly that this is involving a (potential) hack and ask for the IT administrator.
We prefer all correspondence in Dutch, but you can use other languages as well.

We will always answer you, but we do not read our e-mail daily. It may take some days for us to respond to your messages.
When this is an urgent disclosure, calling may be a better option. But the secretary may not fully understand your language or technical terminology.

Anonymity
You may disclose a vulnerability through any communication channel you prefer.
You may remain anonymous.
If you like, we can place your (nick)name on our website to credit you for finding flaws.
If you notify us of a valid vulnerability, and leave us your address, we may send you a small thank-you gift. (Please no DDoS’ing or reporting tons of bogus errors.)

We will notify other organizations when this vulnerability may affect them too.
We will keep you informed about our actions and progress.

(Legal) action
To comply with Dutch and European privacy regulations, we may have to notify victims and report this breach to the Dutch Data Protection Authority. https://autoriteitpersoonsgegevens.nl/en
When the breach involves malicious intent and we believe this has been abused, we may also have to report this breach to the police and take legal action against the abuser.

We will not press charges against you (the discloser), unless:

- You have intentionally broken something
- You have stolen a disproportionate amount of information (like making a copy of all e-mails, while you can prove your vulnerability by just copying a few).
- You have published an exploit method without giving us a chance to patch it first

This policy is based on the Guidelines of the NCSC, for more information please visit:
https://www.ncsc.nl/english/current-topics/responsible-disclosure-guideline.html