THE PROMISE FOUNDATION

For mental health, education and potential realisation

Internet Usage Policy

Policy brief & purpose

Our internet usage policy outlines guidelines for using the Foundation's internet connection, network and equipment. We want to avoid inappropriate or illegal internet use that creates risks resulting in financial loss and reputational damage to the Foundation.

Scope

This policy applies to all our employees, contractors, volunteers, service providers and anyone who access our network and computers.

Internet usage policy elements

What is appropriate internet usage

You are advised to use the Foundation's internet connection for the following reasons:

- To complete your work related duties.
- To seek out information that you can use to improve your work.
- To access your social media accounts, while conforming to our **social media policy.**

We don't want to restrict access to websites of choice, but we expect you to exercise good judgement and remain productive at work while using the internet.

Any use of our network and connection must follow our **confidentiality** and **data protection policy.**

You should:

- Keep your passwords secret at all times.
- Log into your work-related accounts only from safe devices.
- Use strong passwords to log into work-related websites and services.

What is inappropriate internet usage?

You must not use our network to:

- Download or upload obscene, offensive or illegal material.
- Send confidential information to unauthorized recipients.
- Invade another person's privacy and sensitive information.
- Download or upload movies, music and other copyrighted material and software.
- Visit potentially dangerous websites that can compromise the safety of our network and computers.
- Perform unauthorized or illegal actions, like hacking, fraud, buying/selling illegal goods and more.

We also advise you to be careful when downloading and opening/executing files and software. If you are unsure whether a file is safe, you should ask *your supervisor or manager*.

The Foundation may install anti-virus and disk encryption software on our office computers. You may not deactivate or configure settings and firewalls without managerial approval.

The Foundation will not assume any responsibility if personal devices are infected by malicious software, or if personal data are compromised as a result of inappropriate use.

Office-issued equipment
We expect you to respect and protect the Foundation's equipment. Office equipment in this policy includes office-issued phones, laptops, tablets and any other electronic equipment, and belongs to the Foundation.

We advise you to lock your devices at your desk when they are not in use. You are responsible for equipment whenever you take it out of your offices.

Email
You can use your office email account for both work-related and personal purposes as long as you don't violate this policy's rules. You must not use your office email to:

- Register to illegal, unsafe, disreputable or suspect websites and services.
- Send obscene, offensive or discriminatory messages and content.
- Send unauthorized advertisements or solicitation emails.
- Sign up for a competitor's services unless authorized.

The Foundation has the right to monitor office emails. We also have the right to monitor websites that you visit on our computers.

Disciplinary Action
If you don't conform to this internet usage policy you may face disciplinary action. Serious violations will be cause for termination of employment, termination of contract, termination of volunteering engagement, or legal action when appropriate. Examples of serious violations are:

- Using our internet connection to steal or engage in other illegal activities.
- Causing our computers to be infected by viruses, worms or other malicious software.

- Sending offensive or inappropriate emails to our customers, colleagues or partners.

Gideon Arulmani, Director The Promise Foundation
Policy updated 27/7/2020