Marvels and Meltdowns

Internet Usage Policy

Policy brief & purpose

Our employee internet usage policy outlines our guidelines for using our company's internet connection, network and equipment. We want to avoid inappropriate or illegal internet use that creates risks for Marvels and Meltdowns legality and reputation.

Scope

This employee internet usage policy applies to all our employees, contractors, volunteers and partners who access our network and computers.

Employee internet usage policy elements

What is appropriate employee internet usage?

Our employees are advised to use Marvels and Meltdowns internet connection for the following reasons:

- To complete their job duties.
- To seek out information that they can use to improve their work.
- To access their social media accounts, while conforming to our social media policy.

We don't want to restrict our employees' access to websites of their choice, but we expect our employees 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.

Employees should:

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

What is inappropriate employee internet usage?

Our employees mustn't use our network to:

- Download or upload obscene, offensive or illegal material.
- Send confidential information to unauthorised 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 unauthorised or illegal actions, like hacking, fraud, buying/selling illegal goods and more.
- Sign up for a competitor's services unless authorised.

We also advise our employees to be careful when downloading and opening/executing files and software. If they're unsure if a file is safe, they should ask the Marvels and Meltdowns management team.

Marvels and Meltdowns may install anti-virus and disk encryption software on our company computers. Employees may not deactivate or configure settings and firewalls without managerial approval.

We won't assume any responsibility if employee devices are infected by malicious software, or if their personal data are compromised because of inappropriate employee use.

Company-issued equipment

We expect our employees to respect and protect Marvels and Meltdowns equipment. "Company equipment" in this computer usage policy for employees includes company-issued phones, laptops, tablets and any other electronic equipment, and belongs to our company.

We advise our employees to lock their devices in their desks when they're not using them. Our employees are responsible for their equipment whenever they take it out of their offices.

Email

Marvels and Meltdowns employees can use their corporate email accounts for both work-related and personal purposes as long as they don't violate this policy's rules. Employees shouldn't use their corporate email to:

- Register to illegal, unsafe, disreputable or suspect websites and services.
- Send obscene, offensive or discriminatory messages and content.
- Send unauthorised advertisements or solicitation emails.

Marvels and Meltdowns has the right to monitor staff emails. We also have the right to monitor websites employees visit on our computers.

Disciplinary Action

Employees who don't conform to this employee internet usage policy will face disciplinary action. Serious violations will be cause for termination of employment, 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.

Policy issue date: Aug 2017

Policy agreed by the Board of Trustees:

Policy review date: Aug 2018