# Forek Employee 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 our company’s legality and reputation.

## **Scope**

This employee internet usage policy applies to all our employees, students, and guests who access our network and computers.

## **Employee internet usage policy elements**

**What is appropriate employee internet usage?**

Our employees are advised to use our company’s internet connection for the following reasons:

* To complete their job duties (Weekly & Monthly Reports) & Emailing
* To seek out information that they can use to improve their work.
* To access their social media accounts for communication purposes, while conforming to our [social media policy](https://resources.workable.com/social-media-company-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](https://resources.workable.com/confidentiality-company-policy) and [data protection policy](http://resources.workable.com/data-protection-company-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 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 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 Mr IF Oliphant.

Our company 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 as a result of inappropriate employee use.

### **Company-issued equipment**

We expect our employees to respect and protect our company’s equipment. “Company equipment” in this peripheral usage policy for employees includes company-issued phones, laptops, and any other electronic equipment, that belongs to our company.

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

**Emails**

Our employees can use their [corporate email accounts](https://resources.workable.com/email-usage-policy-template) (foreikinstitute.co.za) 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 unauthorized advertisements or solicitation emails.
* Sign up for a competitor’s services unless authorized.

Forek has the right to monitor corporate 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.

## **Indemnity**

**Forek Institute of Technology** provides access to a range wireless network, free of charge, for short-term access to the Company's WiFi network. Network access is provided as a courtesy and convenience to you on an as-is basis. Use of our Network is at your own risk.

This Acceptable Use Policy (this "AUP") governs your access to and use of the Network. Company reserves the right to amend, alter, or modify your conduct requirements as set forth in this AUP at any time.

By agreeing (By Sigature) to the AUP, you accept and agree to be bound and abide by this AUP. If you do not want to agree to this AUP, you must not access or use the Network.

## **Prohibited Use**

You may use the Network only for lawful purposes and in accordance with this AUP. You agree not to use the Network:

• In any way that violates any applicable federal, state, local, or international law or regulation or executive order (including, without limitation, any laws regarding the export of data or software to and from the US or other countries).

• For the purpose of exploiting, harming, or attempting to exploit or harm, minors in any way by exposing them to inappropriate content, asking for personally identifiable information, or otherwise.

• To send, knowingly receive, upload, download, use, or re-use any material which violates the rights of any individual or entity established in any jurisdiction.

• To transmit, or procure the sending of, any advertising or promotional material, including any "junk mail," "chain letter," "spam," or any other similar solicitation.

• To impersonate or attempt to impersonate the Company, a Company employee, another user, or any other person or entity (including, without limitation, by using e-mail addresses or screen names associated with any of the foregoing).

• To engage in any other conduct that restricts or inhibits anyone's use or enjoyment of the Network, or which, as determined by us, may harm the Company or users of the Network or expose them to liability. Additionally, you agree not to:

• Use the Network in any manner that could disable, overburden, damage, or impair the Network or interfere with any other party's use of the Network, including their ability to engage in real time activities through the Network.

• Use any robot, spider, or other automatic device, process, or means to access the

Network for any purpose, including monitoring or copying any Network traffic or resources available on the Network.

Use any manual process to monitor or copy any Network traffic or resources available on the Network or for any other unauthorized purpose without our prior written consent.

• Use any device, software, or routine that interferes with the proper working of the Network.

• Introduce any viruses, trojan horses, worms, logic bombs, or other software or material which is malicious or technologically harmful.

• Attempt to gain unauthorized access to, interfere with, damage, or disrupt any parts of the Network or any server, computer, database, or other resource or element connected to the Network.

• Violate, attempt to violate, or knowingly facilitate the violation of the security or integrity of the Network.

• Otherwise attempt to interfere with the proper working of the Network.

You agree not to use the Network to send, knowingly receive, upload, download, use, or re-use any material which:

• Contains any material that is defamatory, obscene, indecent, abusive, offensive, harassing, violent, hateful, inflammatory, or otherwise objectionable.

• Promotes sexually explicit or pornographic material, violence, or discrimination based on race, sex, religion, nationality, disability, sexual orientation, or age.

• Infringes any patent, trademark, trade secret, copyright, or other intellectual property or other rights of any other person.

• Violates the legal rights (including the rights of publicity and privacy) of others or contains any material that could give rise to any civil or criminal liability under applicable laws or regulations.

• Is likely to deceive any person.

• Promotes any illegal activity, or advocates, promotes, or assists any unlawful act.

• Causes annoyance, inconvenience, or needless anxiety or is likely to upset, embarrass, alarm, or annoy any other person.

• Impersonates any person, or misrepresents your identity or affiliation with any person or organization.

• Involves commercial activities or sales, such as contests, sweepstakes, and other sales promotions, barter, or advertising.

• Gives the impression that they emanate from or are endorsed by us or any other person or entity, if this is not the case.

## **Monitoring & Enforcement**

**Forek**, in its sole discretion, will determine whether your conduct is in compliance with this AUP. We have the right to:

• Discontinue access and/or availability of the Network for any purpose at any time, with or without notice.

• Monitor your use of the Network for any purpose in our sole discretion and as we see fit.

• Take any action we deem necessary or appropriate in our sole discretion if we believe a user's conduct violates this AUP, infringes any intellectual property right or other right of any person or entity, threatens the personal safety of users of the Network or the public, or could create liability for the Company.

• Disclose your identity or other information about you to any third party who claims that material posted by you violates their rights, including their intellectual property rights or their right to privacy.

• Take appropriate legal action, including without limitation, referral to law enforcement, for any illegal or unauthorized use of the Network.

• Terminate or suspend your access to all or part of the Network for any or no reason, including without limitation, any violation of this AUP.

Without limiting the foregoing, we have the right to fully cooperate with any law enforcement authorities or court order requesting or directing us to disclose the identity or other information of anyone who accesses or uses the Network. In addition, you agree to adhere to all applicable social distancing orders in place now or in the future while utilizing the Network and while present in or around Company’s premises.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Date Training Manager

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**ICT Manager**