National Sea Rescue Institute of South Africa "NPC"

Registration No 1967/013618/08

"the Institute"

Internet Use Policy

Approved: 2017
Reviewed: July 2018

NSRI Internet Use Policy

Context and overview

Key details

- Policy prepared by: Ben McCune

Introduction

National Sea Rescue Institute makes internet access available to its employees where relevant and useful for their jobs.

This internet use policy describes the rules governing internet use at the company. It also sets out how staff members are expected to behave when using the internet.

This policy should be read alongside other key policies. The company's data protection and email policies are particularly relevant to staff who use the internet.

Why this policy exists

The internet is a powerful tool that can bring significant benefits to NSRI.

However, it's important every person at the company who uses the internet understands how to use it responsibly, safely and legally.

This internet use policy:

- Reduces the **online security risks** faced by National Sea Rescue Institute
- Lets staff know what they **can and can't do** online
- Ensures employees **do not view inappropriate content** at work
- Helps the company **satisfy its legal obligations** regarding internet use

Policy scope

This policy applies to all staff, contractors and volunteers at National Sea Rescue Institute who use the company's internet on work time.

It applies no matter whether that internet access takes place on company premises, while travelling for business or while working from home.

It applies to use of the internet on any device that is owned by the company, or that is connected to any company networks or systems.

For example, it applies both to an employee using the internet at their desk, and to employees who connect their own tablets or smart phones to the company wireless network.

General internet guidelines

Internet use is encouraged

National Sea Rescue Institute recognises that the internet is an integral part of doing business. It therefore encourages its employees to use the internet whenever such use supports the company's goals and objectives.

For instance, staff members may use the internet to:

- Purchase office supplies
- Book business travel
- Perform competitor or market research
- Identify potential suppliers or partners

There are many valid reasons for using the internet at work and the company certainly allows its employees to explore and take advantage of the internet's many advantages.

Personal internet use

The company also recognises that the internet is embedded in many people's daily lives. As such, it allows employees to use the internet for personal reasons, with the following stipulations:

- Personal internet use should be of a reasonable level and restricted to non-work times, such as breaks and during lunch.

- All rules described in this policy apply equally to personal internet use. For instance, inappropriate content is always inappropriate, no matter whether it is being accessed for business or personal reasons.

- Personal internet use must not affect the internet service available to other people in the company. For instance, downloading large files could slow access for other employees.

Authorised users

Only people who have been authorised to use the internet at National Sea Rescue Institute may do so.

Authorisation is usually provided by an employee's line manager or the company IT department. It is typically granted when a new employee joins the company and is assigned their login details for the company IT systems.

Unauthorised use of the company's internet connection is prohibited.

Employees who use the internet without authorisation — or who provide access to unauthorised people — may have disciplinary action taken against them.

Key areas

Internet security

Used unwisely, the internet can be a source of security problems that can do significant damage to the company's data and reputation.

- Users must not knowingly introduce any form of computer virus, Trojan, spyware or other malware into the company.

- Employees must not gain access to websites or systems for which they do not have authorisation, either within the business or outside it.

- Company data should only be uploaded to and shared via approved services. The IT department can advise on appropriate tools for sending and sharing large amounts of data.

- Employees must not steal, use, or disclose someone else's login or password without authorisation.

Staff members must always consider the security of the company's systems and data when using the internet. If required, help and guidance is available from line managers and the company IT department.

Inappropriate content and uses

There are many sources of inappropriate content and materials available online. It is important for employees to understand that viewing or distributing inappropriate content is not acceptable under any circumstances.

Users must not:

- Take part in any activities on the internet that could bring the company into disrepute.

- Create or transmit material that might be defamatory or incur liability for the company.

- View, download, create or distribute any inappropriate content or material.

  Inappropriate content includes: pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs.

This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.

- Use the internet for any illegal or criminal activities.

- Send offensive or harassing material to others.

- Broadcast unsolicited personal views on social, political, religious or other non-business related matters.

- Send or post messages or material that could damage National Sea Rescue Institute's image or reputation.

Copyright

National Sea Rescue Institute respects and operates within copyright laws. Users may not use the internet to:

- Publish or share any copyrighted software, media or materials owned by third parties, unless permitted by that third party.

- Download illegal copies of music, films, games or other software, whether via filesharing services or other technologies.

Employees must not use the company's equipment, software or internet connection to perform any tasks which may involve breach of copyright law.

Policy enforcement

Monitoring internet use

Company IT and internet resources — including computers, smart phones and internet connections — are provided for legitimate business use.

The company therefore reserves the right to monitor use of the internet, to examine systems and review the data stored in those systems.

Any such examinations or monitoring will only be carried out by authorised staff.

Additionally, all internet data written, sent or received through the company's computer systems is part of official National Sea Rescue Institute records. The company can be legally compelled to show that information to law enforcement agencies or other parties.

Users should always ensure that the business information sent over or uploaded to the internet is accurate, appropriate, ethical, and legal.

Potential sanctions

Knowingly breaching this internet use policy is a serious matter. Users who do so will be subject to disciplinary action, up to and including termination of employment.

Employees, contractors and other users may also be held personally liable for violating this policy.

Where appropriate, the company will involve the police or other law enforcement agencies in relation to breaches of this policy.