Computer Usage Policy

Policy brief & purpose

Our employee Computer 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 Computer Usage Policy applies to all our employees and volunteers who access and use our computers.

Our employees are advised to use our equipment for the following reasons:

- To complete their job duties.
- To seek out information that they can use to improve their work.
- To access the club 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 equipment must follow our Confidentiality and Data Protection policies.

Employees should:

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

Our employees mustn't use our equipment 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 reputation or computers. Perform unauthorised 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 the directors.

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 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 devices when they're not using them. Our employees are responsible for their equipment whenever they take it out of the setting.

Email

Our employees can use the company email accounts for work-related purposes as long as they don't violate this policy's rules.

Employees shouldn't use their company 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.

Our company has the right to monitor emails. We also have the right to monitor websites employees visit on our computers.

Disciplinary Action

Employees who don't conform to this employee Computer 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 equipment 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.

All equipment remains the property of TJ's club (Hampshire) Ltd and will be surrendered when required or when your employment contract is terminated.

This policy was adopted by: TJs Club	Date: May 2020
Signed: J Little	To be reviewed: May 2021

----------✂----------

Computer Usage Policy

Please sign and return to confirm understanding and adherence to this policy

Name of staff member:…….

Signature ……

Date:……