

Always a Sunny Day Internet Café

Acceptable Use Policy

Overview:

Always a Sunny Day Internet Café does not intend to make this establishment any less fun by implementing rules and regulations on what is acceptable use. In fact the pure purpose is to ensure that the café remains a fun environment. By doing this we are ensuring that the users as well as the company is protected from any wrong doing by individuals, either knowingly or unknowingly.

Internet/Intranet related systems, including but not limited to: computer equipment, software, operating systems, storage media, network accounts providing email, WWW browsing, and FTP are the property of Always a Sunny Day Internet Café. Surf wisely big brother IS watching.

Effective security is a team effort and by team we mean employee as well as customer. Always a Sunny Day Internet Café would appreciate full participation from employees and customers in ensuring that security is not breached and nothing but happy surfing occurs. It is the responsibility of every computer user to the user guidelines and to conduct yourselves accordingly.

Why do this?

The overall purpose is to underline acceptable use of all computer equipment at Always a Sunny Day Internet Café. This policy is put in place to protect customers, employees, and Always a Sunny Day Internet Café. Incorrect use exposes everyone to risks including but not limited to: virus attacks, compromise of network systems and services, and legal issues.

The policy applies to both employees and customers of Always a Sunny Day Internet Café. This policy applies to all equipment that is owned or leased by Always a Sunny Day Internet Café.

On with the show..The policy:

1a: Customers will not be able to store any information on Always a Sunny Day Internet Café database. Anyone caught attempting to do so will be asked to leave and never to return. You may bring in your own flash/thumb drives but you may not attempt to access or save information on our database.

1b: Employees while the network administration would like to preserve some level of privacy you will need to understand that anything you store on the company's database is the possession of the company. The before mentioned company being Always a Sunny Day Internet Café. Because of this we cannot guarantee that what you store on Always a Sunny Day Internet Café's database will remain confidential.

2a: Customers are encouraged to and responsible for using good judgment while using Always a Sunny Day Internet Café equipment and internet access. If you are unsure you should be doing something

ask someone. If someone is not available the best option would be to not act, because if it's questionable it is most likely not permitted.

2b: Employee's are responsible for using good judgment regarding reasonableness of personal use. This is a cyber café after all just use your heads when surfing. We do not have separate department policies it is universal and no one is immune to the policy. If you are unsure you should be doing whatever it is you are doing or about to do, ask management. If management is unavailable don't do said act, it's better to NOT act then to act and play ignorant. Ignorance is not an excuse and will not get you out of possible disciplinary action.

3: For security and maintenance purposes Always a Sunny Day Internet Café may monitor equipment, systems and network traffic at anytime.

4: Always a Sunny Day Internet Café reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy. In other words if we suspect misuse we can pull the plug at anytime.

Security and property INFO:

FOR EMPLOYEES:

1. Employee's of Always a Sunny Day Internet Café should take all necessary steps to prevent the releasing of confidential information. Confidential information which include but are not limited to: company private, company strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Take all necessary steps to prevent unauthorized access to any of this information.
2. Keep passwords secure and do not share accounts. You are responsible for your password and account information. If you let someone have access both of you will suffer the consequences so remember this the next time your coworker forgets their password and asks to log in under your information. Passwords will expire every 90 days so hope you are creative.
3. All work stations will be password protected. You will have your own access login/password with administrative rights. There will also be a public access login/password which will not expire every 90 days but could change if necessary. If working on a public station and need to step away you will need to lock that station before leaving it. If you do not disciplinary action will be set which in most cases could lead to immediate termination.
5. Do not join public listserv or "listy" using Always a Sunny Day Internet Café company email address. You may access these using your personal email account.
6. All hosts used by Always a Sunny Day Internet Café employee's whether owned by the employee or Always a Sunny Day Internet Café, shall be continually executing virus-scanning software with a current virus database unless overridden by company policy.

7. Employees must use extreme caution when opening e-mail attachments received from unknown senders. JUST DON'T DO IT. These may contain viruses, e-mail bombs, or Trojan horses. You don't want to be that guy trust me. It's no fun being that guy.

Unacceptable use:

The following activities are prohibited by employees and customers of Always a Sunny Day Internet Café. Some employees may be exempt depending on their legitimate job responsibilities (e.g., admins may have to disable network access to a host of the host is disrupting services).

Under NO circumstances is an employee or customer of Always a Sunny Day Internet Café authorized to engage in any activity that is illegal under local, state, federal, or international law while using Always a Sunny Day Internet Café-owned resources.

The list below was designed to help provide a framework of what is considered unacceptable use.

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Always a Sunny Day Internet Café.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Always a Sunny Day Internet Café or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Using an Always a Sunny Day Internet Café computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
6. Making fraudulent offers of products, items, or services originating from any Always a Sunny Day Internet Café account.
7. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee or customer is not an intended recipient or logging into a server or account that the employee or customer is not expressly authorized to access, unless these duties are within the scope of regular duties. Disruption includes, but it not limited to:

network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

8. Port scanning or security scanning is prohibited.

9. Executing any form of network monitoring while will intercept data not intended or the employee or customer's host, unless this is part of the employee's normal duty.

10. Circumventing user authentication or security or any host, network or account.

11. Interfering with or denying service to any user other than the employee's host (example, denial of service attack).

12. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the internet/intranet/extranet.

13. Providing information about, or lists of, Always a Sunny Day Internet Café employee's to parties outside of Always a Sunny Day Internet Café.

Email and Communication Activities:

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone, or texting, whether through language, frequency, or size of message.

3. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

4. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

5. Use of unsolicited email originating from within Always a Sunny Day Internet Café's networks of other service providers on behalf of, or to advertise, any service hosted by Always a Sunny Day Internet Café or connected via Always a Sunny Day Internet Café's network.

Blogging, Facebooking, Myspaceing, etc...

You can do any of the above here at Always a Sunny Day Internet Café.

Just don't as an employee forget a few important things:

1. Don't forget about the customers while in blog/facebook land. If word gets out that you are ignoring people your privileges will be cut.
2. Be aware that Big Brother is always watching at ALL times.
3. Confidentiality is always a must in regards to Always a Sunny Day Internet Café's interworking. Don't share our secrets and we won't share yours.

4. Employees should not blog/post about how much they dislike their job at their job. Also be aware that we do check your pages when you aren't at work as well. Please restrict the mention of Always a Sunny Day Internet Café in a negative light at all times regardless of where you are.
5. Do not post anything that will tarnish the image of Always a Sunny Day Internet Café. We are friendly here we want to remain that way.
6. Do not post controversial opinions that might reflect on Always a Sunny Day Internet Café. If you feel you need to be controversial don't let people know where you work.

And as always

We reserve the right to change any rules/policies whenever and however we see fit. Any employee found to violate above policies will be subject to disciplinary action which can lead to but not be limited to termination. Customers will have the plug pulled and be asked to leave never to return.