

Stratford-upon-Avon IT Acceptable Use Policy

1.0 Overview

Stratford-upon-Avon College intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Stratford-upon-Avon College established culture of openness, trust and integrity. Stratford-upon-Avon College is committed to protecting Stratford-upon-Avon college's employees, students, partners and the college from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Stratford-upon-Avon College. These systems are to be used for business purposes in serving the interests of the college, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Stratford-upon-Avon College employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Stratford-upon-Avon college. These rules are in place to protect the employee, student and Stratford-upon-Avon College. Inappropriate use exposes Stratford-upon-Avon College to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to students, employees, contractors, consultants, temporaries, and other workers at Stratford-upon-Avon College including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Stratford-upon-Avon College.

4.0 Policy

4.1 General Use and Ownership

1. While Stratford-upon-Avon College's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Stratford-upon-Avon College. Because of the need to protect Stratford-upon-Avon College's network, management cannot guarantee the confidentiality of information stored on any network device belonging to Stratford-upon-Avon College.
2. The College operates within a framework of mutual trust and recognizes that in certain circumstances, particularly when there is a need to communicate urgently, it may be appropriate for employees to send and receive personal emails. However, such reasonable private usage of email must not interfere with employee's work. Excessive private use of email system during working hours will lead to disciplinary action and may in certain circumstances be treated as gross misconduct.
3. The College also recognizes that there may be need for individuals to carry out personal tasks on the Internet whilst at work. However, where such a need arises, employees are required to limit their access to the Internet for personal usage to authorized breaks, lunch breaks or just before or just after normal working hours. Personal use of Internet

during normal working hours may lead to disciplinary action and excessive personal use may in certain circumstances be treated as gross misconduct.

4. Stratford-upon-Avon College recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on encrypting email and documents please contact IT Servicedesk (Ex:3172)
5. For security and network maintenance purposes, authorized individuals within Stratford-upon-Avon College monitor equipment, systems and network traffic at any time.
6. Stratford-upon-Avon College reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines (code of conduct), details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: college private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
3. All PCs, laptops and workstations are secured with a password-protected screensaver with the automatic activation feature set at 60 minutes, or by logging-off (control-alt-delete for Windows users) when the host will be unattended.
4. Because information contained on portable computers is especially vulnerable, special care should be exercised.
5. Postings by employees from a Stratford-upon-Avon College email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Stratford-upon-Avon college, unless posting is in the course of business duties.
6. All hosts used by the employee that are connected to the Stratford-upon-Avon College Internet/Intranet/Extranet, whether owned by the student or staff or Stratford-upon-Avon college, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.
7. Students/Staff must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration

staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Stratford-upon-Avon College authorized to engage in any activity that is illegal under local, state, international law while utilizing Stratford-upon-Avon college owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

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 Stratford-upon-Avon college.
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 Stratford-upon-Avon college or the end user does not have an active license is strictly prohibited.
3. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
4. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
5. Using a Stratford-upon-Avon college computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment.
6. Making fraudulent offers of products, items, or services originating from any Stratford-upon-Avon College account.
7. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is 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 expressly prohibited unless prior notification to Computing Services department is made.
9. Executing any form of network monitoring which will intercept data not intended for the student/staff host, unless this activity is a part of the employee's normal job/duty.
10. Circumventing user authentication or security of any host, network or account.

11. Interfering with or denying service to any user other than the employee's host (for 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, Stratford-upon-Avon college student or staff to parties outside Stratford-upon-Avon College.

Email and Communications 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 paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. 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.
5. Creating or forwarding "chain letters".
6. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.4. Internet Use Monitoring and Filtering

1. Stratford-upon-Avon College Computing Services department shall monitor Internet use from all computers and devices connected to the College network. For all traffic the monitoring system must record the source IP Address, the date, the time, the protocol, and the destination site or server. Where possible, the system should record the User ID of the person or account initiating the traffic. Internet Use records must be preserved for 180 days.
2. General trending and activity reports will be made available to any employee as needed upon request to the Computing Services Department. Computer Security Incident Response Team/Infrastructure Team (CSIRT) members may access all reports and data if necessary to respond to a security incident. Internet Use reports that identify specific users, sites, teams, or devices will only be made available to associates outside the CSIRT upon written or email request to Director of Computing Services from a Human Resources Representative.
3. The Information Technology Department shall block access to Internet websites and protocols that are deemed inappropriate for Stratford-upon-Avon College's corporate environment. The following protocols and categories of websites should be blocked:
 - Adult/Sexually Explicit Material

- Advertisements & Pop-Ups
 - Chat and Instant Messaging
 - Gambling
 - Hacking
 - Illegal Drugs
 - Intimate Apparel and Swimwear
 - Peer to Peer File Sharing
 - Personals and Dating
 - Social Network Services
 - SPAM, Phishing and Fraud
 - Spyware
 - Tasteless and Offensive Content
 - Violence, Intolerance and Hate
4. The Computing Services Department shall periodically review and recommend changes to web and protocol filtering rules. The Executive Team shall review these recommendations and decide if any changes are to be made.
 5. If a site is mis-categorized, staff may request the site be un-blocked by submitting a ticket to the IT Service desk using an online form published on the college Intranet. IT Servicedesk will review the request and un-block the site if it is mis-categorized. Staff/Students may access blocked sites with permission if appropriate and necessary for business purposes. If staff needs access to a site that is blocked and appropriately categorized, they must will in the online filtering request form and relevant line manager will authorise the request and pass it on to IT Servicedesk. Computing Services will unblock that site or category for that associate only.
 6. Network security analyst will periodically review Internet use monitoring and filtering systems and processes to ensure they are in compliance with this policy. Any student or staff found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.4. Blogging

1. Blogging by employees/ students , whether using Stratford-upon-Avon College's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use Stratford-upon-Avon college 's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Stratford-upon-Avon college 's policy, is not detrimental to Stratford-upon-Avon college's best interests, and does not interfere with an employee's regular work duties. Blogging from Stratford-upon-Avon College 's systems is also subject to monitoring.
2. Staff & students are prohibited from revealing any Stratford-upon-Avon college confidential or proprietary information, trade secrets or any other material covered by Stratford-upon-Avon college Confidential Information policy when engaged in blogging.
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Stratford-upon-Avon College and/or any of its students/staff. Students & staff are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Stratford-upon-Avon college's Non-Discrimination and Anti-Harassment policy.

4. Staff & students may also not attribute personal statements, opinions or beliefs to Stratford-upon-Avon College when engaged in blogging. If a staff member or a student is expressing his or her beliefs and/or opinions in blogs, the staff member or a student may not, expressly or implicitly, represent themselves as an employee or representative of by Stratford-upon-Avon college.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, by Stratford-upon-Avon college's trademarks, logos and any other Stratford-upon-Avon college intellectual property may also not be used in connection with any blogging activity

5.0 Enforcement

Any a staff member is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or in the case of students, expulsion from the college.

6.0 Definitions

Term	Definition
-------------	-------------------

<i>Blogging</i>	Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.
-----------------	--

<i>Spam</i>	Unauthorized and/or unsolicited electronic mass mailings.
-------------	---

<i>Internet Filtering</i>	Using technology that monitors each instance of communication between devices on the corporate network and the Internet and blocks traffic that matches specific rules
---------------------------	--

<i>User ID</i>	User Name or other identifier used when an associate logs into the corporate network.
----------------	---

<i>IP Address</i>	Unique network address assigned to each device to allow it to communicate with other devices on the network or Internet.
-------------------	--

<i>SMTP mail</i>	Simple Mail Transfer Protocol. The Internet Protocol that facilitates the exchange of messages between Internet mail servers.
------------------	---

<i>Peer to Peer File</i>	
--------------------------	--

Sharing – Services or protocols such as BitTorrent and Kazaa that allow Internet connected hosts to make files available to or download files from other hosts.

Social Networking Services – Internet sites such as Myspace and Facebook that allow users to post content, chat, and interact in online communities.

SPAM – Unsolicited Internet Email. SPAM sites are websites link to from unsolicited Internet mail messages.

Phishing – attempting to fraudulently acquire sensitive information by masquerading as a trusted entity in an electronic communication.

Hacking – Sites that provide content about breaking or subverting computer security

7.0 Revision History

13th November 2008 - Draft Completed , Vamsi Bodepudi

2nd June 2009 - Version 2 - Send for Approval

21 September 2010 - Policy Updated