

StaffShare® Good Behaviour Agreement

SS.GBA.Mar.10.DL

1. Introduction

The purpose of this agreement is to establish acceptable and unacceptable behaviour with regard to the use of resources at www.staffshare.co.uk, or on behalf of, StaffShare Ltd. (herein “StaffShare” or “company”). Resources covered include, but are not limited to hardware and software assets, websites, brand, service provision and IPR.

StaffShare provides ‘skill exchange services’ and must manage its resources responsibly to maintain its established culture of quality, confidentiality, integrity and availability (QCIA). This agreement requires those that utilise these resources, for example as ‘Members’ and any third party operators, to comply with company policies.

2. Scope

All contractors, partners, consultants, temporary and other workers at or for StaffShare, including all personnel affiliated with third parties must adhere to this agreement. This agreement applies to resources owned, licensed or leased by StaffShare.

StaffShare must approve any exceptions to this agreement in advance through liaison with StaffShare’s management team.

3. Agreement Statement

3.1. General Requirements

You are responsible for exercising good judgment regarding appropriate use of StaffShare resources in accordance with StaffShare policies, standards, and guidelines. StaffShare resources may not be used for any unlawful or prohibited purpose.

For security, compliance, and maintenance purposes, authorised personnel may monitor and audit equipment, systems, and network traffic. If devices interfere with other devices or users on the StaffShare network they may be disconnected without notification.

Do not interfere with corporate device management or security system software, including, but not limited to, Symantec antivirus, Antigen, Forefront, HP SIM, Microsoft Operations Manager and System Centre Operations Manager.

You are responsible for maintaining all client communications in line with our brand guidelines, this covers style of communication e.g. no jargon, and use of logos, email footers etc.

Acting on behalf of – where you cannot use StaffShare assets to perform illegal activity this also extends to non- StaffShare assets trading under or acting on behalf of StaffShare.

3.2. System Accounts

You are responsible for the security of data, accounts, and systems under your control. Keep passwords secure and do not share account or password information with anyone unless strictly under your control and authority, including other personnel, family, or friends. Providing access to Member’s areas to another individual, both deliberately or through failure to protect access, is a violation of this agreement and may result in access being withdrawn.

You must maintain system-level and user-level passwords in accordance with StaffShare’s log-on and password policy.

You must ensure through legal or technical means that proprietary information remains within the control of StaffShare at all times. Conducting StaffShare business that results in the storage of proprietary information on personal or non-StaffShare controlled environments, including devices maintained by a third party with whom StaffShare does not have a contractual agreement, is prohibited.

3.3. Computing Assets

You are responsible for ensuring the protection of assigned StaffShare assets that includes the use of computer cable locks and other security devices.

All PCs, PDAs, laptops, and workstations must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

3.4. Minimum Client Requirements

Devices that connect to the StaffShare network must comply with the following minimum standards:

3.4.1. All Clients

- Antivirus installed and maintained at the latest signature level
- Operating system patched to the latest security level to prevent exploitation of known vulnerabilities
- Connect only when necessary and for business purposes only; Internet access is restricted through the VPN client for this reason.

3.4.2. Windows Client - Standards

- Windows XP Service Pack 3 or Windows Vista SP1 clients only
- Windows update enabled and machine patched and maintained at the latest release level
- Windows firewall enabled or a third-party solution installed
- *Optional, but preferred:* Antispyware installed and maintained at the latest signature level

Should you not have antivirus available on your machine the following vendors are suitable:

Premium antivirus solutions:

- www.mcafee.com
- www.symantec.com
- www.f-secure.com

NB: Acceptable freeware antivirus is available from www.grisoft.com (AVG).

All of these providers offer a wider security solution including a firewall client and anti-spyware software available as a package.

3.4.3. Apple Macintosh – Standards

- Mac OS X updated to the latest release and patch level.
- Built in firewall enabled or a third-party solution installed

Optional, but preferred: Antispyware installed and maintained at the latest signature level

Should you not have antivirus available on your machine the following vendors are suitable:

Premium antivirus solutions:

- www.mcafee.com (Virex)
- www.symantec.com (Norton Antivirus)

These providers offer a wider security solution including firewall client and anti-spyware software available as a package.

3.4.4. Linux - Standards

Linux comes in numerous 'flavours' at over 100 currently. Common flavours in use are Mandrake, Red Hat, Debian, SuSE, Gentoo and Caldera.

- Linux operating system should be patched to the latest security level
- Built in firewall enabled or a third-party solution installed
- *Optional, but preferred:* Antispyware installed and maintained at the latest signature level

Should you not have antivirus available on your machine www.pandasoftware.com produce a Linux solution that also includes antispyware and firewall solutions.

3.5. Network Use

You are responsible for the security and appropriate use of StaffShare network resources under your control. Using StaffShare resources for the following is strictly prohibited:

1. Causing a security breach to either StaffShare or other network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorised; circumventing user authentication on any device; or sniffing network traffic.
2. Causing a disruption of service to either StaffShare or other network resources, including, but not limited to, ICMP floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes.
3. Introducing "honey pots", "honey nets", or similar technology on the StaffShare network.
4. Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software.
5. Exporting or importing software, technical information, encryption software, or technology in violation of international or regional export control laws.
6. Use of the Internet or StaffShare network that violates this agreement or local laws.
7. Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and key-loggers
8. Port scanning or security scanning on a production network unless authorized in advance by Technical Management

3.6. Electronic Communications

The following are strictly prohibited:

1. Inappropriate use of communication vehicles and equipment, including, but not limited to, supporting illegal activities, and procuring or transmitting material that violates StaffShare policies against harassment or the safeguarding of confidential or proprietary information.
2. Sending Spam via e-mail, text messages, pages, instant messages, voice mail, or other forms of electronic communication.
3. Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.
4. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
5. Use of a StaffShare e-mail or IP address to engage in conduct that violates StaffShare policies or guidelines. Posting to a public newsgroup, bulletin board, or listserv with a StaffShare e-mail or IP address represents StaffShare to the public; therefore, you must exercise good judgment to avoid misrepresenting or exceeding your authority in representing the opinion of the company.

4. Specific Requirements

The following requirements must be followed at all times:

1. Any customer data held must be kept securely using industry best practise and comply with all statutory and regulatory requirements.
2. Any sensitive customer data should not be accessed from publicly accessible machines such as libraries, internet cafes and similar locations.
3. StaffShare Member data must not ever be stored on portable storage devices such as USB memory sticks or writable CD's.

5. Acceptance

By signing the following, you accept the content of this agreement and will make every possible attempt to adhere to the requirements herein. Inappropriate use as defined within this agreement will not be tolerated and careless or malicious activity could result in the removal of access rights.

Member Name	
Member Representative Name	
Date	
Signed	

StaffShare Representative Name	
Date	
Signed	