Taboola's Acceptable Use Policy

1) Overview

Acceptable use, as it refers to Taboola.com Ltd., its subsidiaries and affiliates (collectively, "Taboola", or the "Company"), is a statement of the guidelines created for the purpose of defining the proper practices in relation to the use of Taboola's technology resources. These resources may include, but not be limited to (i) the use of the internet, computers, mobile devices, printing devices and electronic communication platforms such as email and social media platforms, (ii) data security, and (iii) confidentiality. This policy also outlines the sanctions and measures that may be taken in the event that the rules contained herein are violated.

Taboola's intentions for publishing a policy gathering said guidelines and sanctions (hereinafter referred to as "Acceptable Use Policy") are not to impose restrictions that are contrary to Taboola's established culture of openness, trust, and integrity. Taboola is committed to protecting Taboola's employees, partners and the Company from illegal or damaging actions by individuals, either knowingly or unknowingly.

2) Purpose

The purpose of this policy is to outline the acceptable use of computer and information technology ("IT") equipment at Taboola. These rules are in place to protect all individuals working at or on behalf of Taboola. Inappropriate use exposes Taboola to risks including virus attacks, compromise of network systems and services, and legal issues.

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

3) Scope

This Acceptable Use Policy pertains to the security and use of all Taboola's information and IT equipment. It also includes guidelines regarding the use of email, internet, voice and mobile IT equipment, storage media, and network-shared folders, including when accessed using your personal devices that you have chosen to use for work (when authorized by Taboola). These systems are to be used for business purposes in serving the interests of the Company, and of our clients and customers in the course of normal operations.

This policy applies to any individual/person, which is either an employee of Taboola, a contractor who provides services to Taboola and/or any of its employees or anyone who acts on such contractors' behalf, or any agent who acts on behalf of Taboola (hereinafter: "you"

or "Policy Subject(s)". This policy applies to all information, in whatever form, relating to Taboola's business activities worldwide, and to all information handled by Taboola. It also covers all IT facilities operated by Taboola's or on its behalf.

4) Policy

a) General Use and Ownership

i) All Taboola proprietary information stored on electronic and computing devices whether owned or leased by Taboola, the employee, or a third party, remains the sole property of Taboola. You must ensure through legal or technical means that proprietary information is protected in accordance with the Internal IT Policies.

ii) You have a responsibility to promptly report an actual or potential theft, loss or unauthorized disclosure of Taboola proprietary information.

iii) You may access, use or share Taboola proprietary information only to the extent it is authorized and necessary to fulfil your job.

iv) You are responsible for exercising good judgment regarding the personal use of IT systems, such as devices, software, SaaS accounts or cloud services. The guidelines concerning personal use of Taboola's IT systems can be found in the internal IT policies Brain space, available at https://brain.taboola.com/display/IITP ("Internal IT Policies"). If there is any uncertainty, you should consult their supervisor or manager.

v) For security and network maintenance purposes, authorized individuals within Taboola may monitor equipment, systems, and network traffic at any time, per Taboola's Internal IT Policies, including when accessed using your personal devices that you have chosen to use for work (when authorized by Taboola).

vi) Taboola reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

b) Security and Proprietary Information

i) System level and user level passwords must comply with the Internal IT Policies. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

ii) All company owned computing devices and your personal devices that you have chosen to use for work (when authorized by Taboola) must be protected by an MDM (Mobile Device Management) system. The MDM allows IT to control

Taboola's laptops and company owned phones remotely, control the encryption of the device, wipe the device (if needed) remotely, and apply the organization protection and password policy on each device.

iii) All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 15 minutes or less. You must lock the screen or log off when the device is unattended.

iv) Postings by employees or authorised contractors and third parties from a Taboola email address to newsgroups, professional networks, or social media sites should be strictly professional and include only necessary facts, no personal opinions, political agenda, client information, or personal information, and shall be subject to Taboola's Social Media Policy, available at https://brain.taboola.com/display/LEGAL/Social+Media+Policy ("Social Media Policy").

v) You must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware. When in doubt, you should forward the email security@taboola.com.

c) Unacceptable Use

The following activities are, in general, prohibited. Some of the Policy Subjects 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 Taboola authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing Taboola-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.

i) System and Network Activities

The following activities are strictly prohibited:

(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 Taboola.

(2) Unauthorized copying of copyrighted or confidential material including, but not limited to, data from databases, data from servers, log files, digitization, and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Taboola or the end user does not have an active license.

(3) Accessing any person's computer or computer system, software, or data without their knowledge and consent; breaching the security of another user; or attempting to circumvent the user authentication or security of any host, network, or account. This includes, but is not limited to, unauthorizedly accessing classified data, logging into or using a server or account you are not expressly authorized to access, or probing the security of other hosts, networks, or accounts.

(4) Accessing data, a server or an account for any purpose other than conducting Taboola related business.

(5) Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws. Management should be consulted prior to export of any material that is in question.

(6) Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

(7) Revealing your account password to others or allowing use of your account by others. This includes family and other household members.

(8) Using a Taboola device 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.

(9) Making fraudulent offers of products, items, or services originating from any Taboola account.

(10) Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

(11) Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the Policy Subject is not an intended recipient or logging into a server or account that the Policy Subject 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.

(12) Port scanning or security scanning is expressly prohibited unless prior notification to Taboola is made.

(13) Executing any form of network monitoring which will intercept data not intended for the Policy Subject's host, unless this activity is a part of the Policy Subject’s normal job/duty.

(14) Circumventing user authentication or security of any host, network or account.

(15) Introducing honeypots, honeynets, or similar technology on the Taboola network.

(16) Interfering with or denying service to any user other than the Policy Subject's host (for example, denial of service attack).

(17) 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.

(18) Providing information about, or lists of, Taboola employees to parties outside Taboola without Taboola Security Officer's prior approval.

ii) Email and Communication Activities

Taboola email addresses should be used primarily for Taboola related business and activities. Taboola's email addresses should not be used in conjunction with personal services.

Personal email or communications (such as WhatsApp, Telegram and others) should not be used for work related communications.

When using company resources to access and use the internet, users must realize they represent the Company. Whenever Policy Subjects state an affiliation to the Company, they must be strictly professional and include only necessary facts, no personal opinions, political agenda, client information, or personal information.

The following activities are prohibited:

(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 or telephone. Harassment includes sending messages that contain profane or offensive language, sending frequent unsolicited messages, or sending extremely lengthy 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", "Ponzi" or other "pyramid" schemes of any type.

(6) Use of unsolicited email originating from within Taboola's networks of other intranet/extranet service providers on behalf of, or to advertise, any service hosted by Taboola or connected via Taboola's network.

(7) Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

iii) Blogging and Social Media

(1) Blogging by employees, or authorised contractors and third parties, whether using Taboola's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Acceptable Use Policy. Limited and occasional use of Taboola's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate any of Taboola's policies (including, but limited to, Taboola's Social Media Policy), is not detrimental to Taboola's best interests, and does not interfere with the Policy Subjects' regular work duties.

(2) Taboola's Internal IT Policies regarding confidential information also apply to blogging. As such, Policy Subjects are prohibited from revealing any of Taboola's confidential or proprietary information, trade secrets, or any other material covered by any of Taboola's policies.

(3) Policy Subjects shall not engage in any blogging that may harm or tarnish the image, reputation, and/or goodwill of Taboola and/or any of its employees. Policy Subjects are also prohibited from making any discriminatory, disparaging, defamatory, or harassing comments when blogging or otherwise engaging in any conduct prohibited by any of Taboola's Internal IT Policies and Taboola Social Media Policy.

(4) Policy Subjects may also not attribute personal statements, opinions, or beliefs to Taboola when engaged in blogging. If a Policy Subject is expressing his or her beliefs and/or opinions in blogs, the Policy Subject may not, expressly or implicitly, represent themselves as an employee or representative of Taboola. Policy Subjects assume any and all risk associated with blogging.

(5) Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, Taboola's trademarks, logos, and any other Taboola intellectual property may also not be used in connection with any blogging activity.

5) Policy Compliance

i) Compliance Measurement

Taboola will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

ii) Exceptions

Any exception to the policy must be approved by Taboola in advance.

iii) Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment in accordance with the applicable employment law, regardless of Taboola's right to seek indemnification from you in case your actions or omissions result in losses to Taboola. Notwithstanding other rights Taboola might have, a violation of this Policy by a contractor or a third party will constitute a material breach of the engagement with Taboola, and will allow Taboola to immediately terminate the engagement with such contractor or third party.

6) Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:

https://www.sans.org/security-resources/glossary-of-terms/

a) Blogging

b) Honeypot

c) Honeynet

d) Proprietary Information

e) Spam

7) Revision History

Date of Change	Responsible	Summary of Change
December 18, 2019	Ariel Pisetzky	Yearly review & adding information about the MDM system.
January 29th, 2020	Ariel Pisetzky	Spelling correction
February 17th, 2020	Legal & Ariel Pisetzky	Minor updates
April 23rd 2020	Legal & Ariel Pisetzky	Minor updates & clarification on use of personal devices and communications

October 27th 2021	Legal	Clarification to the Scope & adding reference to Taboola's Social Media Policy