12.0 Acceptable Use

12.1 Acceptable Use Policy
12.2 Acceptable Use Form

12.1 Acceptable Use Policy

1. Overview

This Acceptable Use Policy governs the use and security of all information and computer equipment from Watershed Public Charter School, Inc. (WPCS, Inc.) It also covers the use of email, the internet, voice and any computing equipment.

This policy applies to all information, in any form, relating to the business activities of WPCS, Inc., and to all information processed by WPCS, Inc. about other organizations with which it deals.

This policy also covers all IT and information communication facilities operated by or on behalf of WPCS, Inc.

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 Watershed. These systems are to be used for business purposes in serving the interests of the entity and those we serve in the course of normal operations.

WPCS, Inc. is committed to protecting its employees, partners and the entity from illegal or damaging actions by individuals, either knowingly or unknowingly.

It is the responsibility of every WPCS, Inc. account user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment and internet accounts through Watershed Public Charter School, Inc. These rules are in place to protect the user and WPCS, Inc. Inappropriate use exposes WPCS, Inc. to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

This policy applies to employees of the Watershed Public Charter School, Inc., contractors, consultants, temporary employees, volunteers and other workers commissioned by WPCS, Inc., including all personnel affiliated with third parties. This policy applies to all equipment owned or leased by WPCS, Inc.

It also applies to the use of information, electronic and computer equipment and network resources to conduct business activities or interact with internal networks and business systems, whether owned or leased by WPCS, Inc., the employee or a third party.

All employees, contractors, consultants, temporary employees and other workers of WPCS, Inc. and its subsidiaries are responsible for exercising judgment with respect to the appropriate use of information, electronic devices and network resources in accordance with WPCS, Inc. policies and standards and local laws and regulations.

4. Individual's Responsibility
5.
Access to the WPCS, Inc. IT systems (e.g., Google Drive, etc.) is controlled by the use of user IDs, passwords and/or tokens. All user IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the WPCS, Inc. IT systems.

Individuals must not:

- Allow anyone else to use their user ID/token and password on any WPCS, Inc. IT system
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access WPCS, Inc.'s IT systems
- Leave their password unprotected (e.g., writing it down)
- Perform any unauthorized changes to WPCS, Inc.'s IT systems or information
- Attempt to access data that they are not authorized to use or access
- Exceed the limits of their authorization or specific business need to interrogate the system or data
- Store WPCS, Inc. data on any non-authorized WPCS, Inc. equipment
- Give or transfer WPCS, Inc. data or software to any person or organization outside WPCS, Inc. without the authority of WPCS, Inc. Including but not limited to the information stored on the organization's Google Drive.

6. Internet And Email

The use of the internet and email of WPCS, Inc. is intended for professional purposes only. All individuals granted use of a WPCS email address (including but not limited to staff and WPCS volunteers) are therefore responsible for their actions on the internet as well as when using email systems. Users must not:

- Use the internet or email for harassment or abuse
- Use blasphemies, obscenities or disrespectful remarks in communications
- Access, upload, send or receive data (including images) that WPCS, Inc. considers offensive in any way, including sexually explicit, discriminatory, defamatory or libelous material
- Use of the internet or email to make personal gains or run a personal business

- Use the internet or email to play games or for gaming purposes
- Use email systems in a way that could affect their reliability or efficiency, for example by distributing chain letters or spam
- Place on the internet any information relating to WPCS, Inc., modify any information concerning it or express any opinion on WPCS, Inc., unless they are expressly authorized to do so
- Send sensitive or confidential information that is not protected to the outside world
- Use of unsolicited email originating from within WPCS, Inc.'s networks of other internet/intranet/extranet service providers on behalf of, or to advertise, any service hosted by WPCS, Inc. or connected via its network
- Forward business email to personal email accounts (for example, Gmail account)
- Make official commitments by internet or email on behalf of WPCS, Inc., unless authorized to do so
- Download copyrighted material such as music media files, films and videos (non-exhaustive list) without appropriate approval
- In any way, violate copyright, database rights, trademarks or other intellectual property rights
- Download any software from the internet without the prior consent of WPCS, Inc.
- Connect WPCS, Inc. devices to the internet using non-standard connections

<u>Volunteers granted use of a WPCS email address must not</u>:

- Represent themselves as staff of WPCS, Inc.
- Enter into any agreements on behalf of WPCS, Inc.
- Share information contained on the Google Drive

7. General Use Ownership

WPCS, Inc. proprietary information stored on electronic and computing devices--whether owned or leased by WPCS, Inc--remains the sole property of WPCS, Inc. You must ensure through legal or technical means that proprietary information is protected in accordance with the data protection standards.

You have a responsibility to promptly report the theft, loss or unauthorized disclosure of WPCS, Inc. information.

You may access, use or share WPCS, Inc. proprietary information only to the extent it is authorized and necessary to perform the tasks assigned to you.

Users are responsible for exercising their good judgment as to the reasonableness of personal use. Users should consult the Executive Director in the event of uncertainty.

WPCS, Inc. reserves the right to periodically audit networks and system to ensure compliance with this policy.

8. Blogging And Social Media

Blogging by employees, whether using WPCS, Inc.'s property and systems or personal computer systems, is also subject to the terms and restrictions set out in this policy. The limited and occasional use of WPCS, Inc.'s systems for bloggins is acceptable, provide that it is done in

a professional and responsible manner, does not otherwise violate WPCS, Inc.'s policy, does not prejudice the best interests of WPCS's, Inc. and does not interfere with the user's normal duties. Blogging from WPCS, Inc.'s systems is also subject to monitoring.

Users shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of WPCS, Inc. and/or any of its employees. Users are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or posting on social media.

Employees may also not attribute personal statements, opinions, or beliefs to WPCS, Inc. when engaged in blogging or posting on social media.

9. Security And Proprietary Information

All access to the entity's computer network must be protected by passwords.
It is prohibited to allow access to another person, either deliberately or by failing to adequately protect the right of access that has been granted.

All computer devices shall be protected by a password-protected screen saver with an automatic activation function set to 10 minutes or less. You must lock the screen or disconnect when the unit is unattended.

Messages posted by users from a WPCS email address on forums should contain a warning that the opinions expressed are strictly theirs and not necessarily those of WPCS, unless the message is posted in the course of professional duties.

Employees must exercise extreme caution when opening attachments to emails received from unknown senders, which may contain malware.

Users must not remove or disable anti-virus software.

Attempt to remove virus-infected files or clean up an infection, other than by the use of approved WPCS anti-virus software and procedures.

10. WORKING OFF-SITE
It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Working off-site must be in line with any WPCS remote working policy.
- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely. Laptop encryption must be used.
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

11. Unacceptable Use

The following activities are prohibited. Under no circumstances is a user of WPCS, Inc. authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing WPCS-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.

The following activities are strictly prohibited, with no exceptions:

- Infringements of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or by similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” products or other software the use of which is not authorized by WPCS, Inc.
- 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 WPCS, Inc. or the end user holds no active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
- Making fraudulent offers of products, items, or services originating from any WPCS, Inc. account.
- Making security breaches or disruptions of network communication.
- Executing any form of network monitoring which will intercept data not intended for the employee’s host, unless this activity is a part of the employee’s normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the employee’s host (for example, denial of service attack).
- 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.
- Providing information about, or lists of, employees and volunteers to parties outside WPCS, Inc.

12.2 User Agreement Form

I acknowledge that I have received a copy of Watershed Public Charter School’s Acceptable Use Policy. I have read and understand the policy. I understand that, if I violate the policy, I may be subject to disciplinary action, including termination of my duties. I further understand that I will contact my supervisor or the Executive Director of Watershed or Watershed Board Secretary if I have any questions about any aspect of the policy.

Dated: _____

EMPLOYEE COMPANY

_____	_____
Authorized Signature	Authorized Signature
_____	_____
Print Name and Title	Print Name and Title