

Mindbridge Technology Usage Policy

V.1.0

Last revised: 6 March 2018

I. Introduction

The Mindbridge Foundation (“Mindbridge”) establishes this policy to lay out acceptable and unacceptable usage of electronic devices and other technological assets under its possession. Mindbridge offers these assets to assist projects with their work.

II. Administration

The Mindbridge Board of Directors (“Board”) or a person(s) designated by the Board (“Designee”) shall act as the enforcing body. All requests to check out or use technology assets shall be done in writing, and approved by either the Board or a Designee. The request shall also indicate that they have read and aware of the Technology Usage Policy, and agree to abide by it and any other policies that govern usage of Mindbridge assets.

Members are responsible for exercising good judgment regarding what is considered appropriate usage in line with policies and guidelines. The Board or Designee reserves the right to revoke or restrict access to technology assets of anyone who violates this or other policies.

III. Inventory Requirements

The Board or Designee shall keep an inventory of all technology assets. Assets that require regular updates may be recalled by the Board or Designee to ensure that updates are installed, or may permit members to install those updates in their stead.

Members who have technology assets in their possession are required to either return their assets to the Mindbridge storage locker, or contact the Board or Designee with current status of those assets. These updates should be made before the start of the next fiscal year.

IV. Access Requirements

Certain assets may require a password or other credentials to access, or their software may require credentials. Only members who are authorized to access those systems or software may do so; sharing of credentials is forbidden. If someone needs access to a system or software, it should be approved by the Board or Designee.

Members who have technology assets in their possession are required to ensure that they are properly secured. This includes logging out or locking of software when not in use to prevent unauthorized access, securing objects physically so they can't be stolen, and storing them in a secure manner so that they aren't damaged.

V. Software Requirements

The Board or Designee shall establish a list of acceptable software for technology assets. Computers and laptops should which will be connected to the internet and contain sensitive

Mindbridge information should have an active antivirus software installed. To ensure that software stays up to date, the Board or Designee may request assets that are checked out be returned so that updates can be performed.

Members are forbidden from installing their own software without the permission of the Board or Designee. The installation of pirated or unlicensed software is also forbidden.

VI. Other Restrictions

Technology assets are to be used to further the interests and goals of Mindbridge or its projects. As such all work done with those assets are considered the sole property of the Mindbridge. The personal use of Mindbridge assets is strictly forbidden unless written approval is granted by the Board.

Unless part of a sanctioned work, technology assets should not be used to view, display, or store material that would be considered inappropriate for minors. If a sanctioned work is to be done, that should be noted in the usage request to the Board or Designee. After that work has been completed, any material related to that work should be removed from that technology asset, or the Board or Designee should be notified that it remains on that asset.