PITZER COLLEGE

OFFICE OF STUDENT AFFAIRS

WIFI HOT SPOT LOAN AGREEMENT

I understand and agree that that:

___ I am responsible for returning this hot spot by no later than 5:00 p.m. the date indicated below to the Office of Student Affairs (Scott Hall 120).

___ If I fail to return the hot spot on time to the Office of Student Affairs (Scott Hall 120), I will be fined $10 per day, up to the total cost of a replacement hot spot.

___ If, after a Pitzer IT staff inspection, it is determined that I damaged the hot spot, I will be charged repair or replacement costs.

___ If after an Pitzer IT staff inspection, it is determined that I did not return all cables or accessories, I will be charged replacement costs.

___ If I tamper with the equipment, I will be charged to repair or replace the hot spot and any cables or accessories and may also be subject to disciplinary action.

___ Pitzer College is not responsible for damage to external drives or any other devices plugged into the hot spot, if applicable.

___ I agree to abide by The Claremont Colleges Policy Regarding Appropriate Use of Campus Computing and Network Resources which can be found on the back (second page) of this form and online in the Pitzer College Student Handbook.

I understand that by borrowing this hot spot, I am responsible for its return. If the hot spot is lost or stolen while on loan to me, I am responsible for the entire replacement cost of the equipment.

_____

Printed Name Signature Date

Return Date _____

The Claremont Colleges Policy Regarding Appropriate Use of Campus Computing and Network Resources

An overall guiding mission of The Claremont Colleges is education in an environment where the free exchange of ideas is encouraged and protected. The Claremont Colleges make available computing and network facilities (CNF) resources for use by the Colleges' students, faculty and staff. These services are provided for educational purposes and to carry out the legitimate business of the Colleges. The Colleges and members of the college communities are expected to observe Federal, State and local laws that govern computer and telecommunications use, as well as the Colleges' regulations and policies.

Computing and network facilities resources users are required to use these resources within the Colleges' standards of conduct. Individuals with expert knowledge of information systems or who make extensive use of these facilities, or with a position of trust regarding these facilities will be held accountable to a higher standard.

Responsible, considerate and ethical behavior expected by the Colleges extends to use of computing and network facilities resources and networks throughout the world to which electronic access has been provided. These CNF resources include but are not limited to:

Computers and associated peripheral devices	Campus video cable	Classroom presentation systems
Data networking equipment systems, including remote and wireless access	Computer software	Voice messaging equipment
Electronically stored institutional data and messages	All other similar resources owned, controlled and/or operated by the Colleges and Services to maintain these resources.	

Ownership: The Colleges retain absolute ownership rights of the CNF resources. Such resources are not owned by a department or by any individual. CNF resources leased, licensed, or purchased under research contracts or grants, are administered under the terms of this policy for as long as they remain within the lawful possession or control of the Colleges. CNF resources provided to on-campus residences are also owned, operated and provided by the Colleges.

Access to Resource: Access to CNF resources is a privilege, which is allowed only to the Colleges' authorized personnel and students. All users must understand and abide by the responsibilities that come with the privilege of use. Such responsibilities include, but are not limited to, the following:

1. You must understand and comply with all applicable federal, state and local laws.
2. You must not intentionally seek information about, browse, copy, or modify non-public files belonging to other people, whether at a Claremont College or elsewhere.
3. You are authorized to use only computer resources and information to which you have legitimately been granted access. Sharing your passwords with others is expressly forbidden. Any attempt to gain unauthorized access to any computer system, resource or information is expressly forbidden. If you encounter or observe a gap in system or network security, immediately report the gap to the manager of that system.
4. Each College's Policy on Harassment applies as equally to electronic displays and communications as to the more traditional (e.g., oral and written) means of display and communication.
5. Messages, sentiments and declarations sent as electronic mail or postings must meet the same standards for distribution or display as physical (paper) documents would on college property.
6. Unsolicited mailings and unauthorized mass mailings from campus networks or computing resources (i.e., "spam") are prohibited. Each campus may have specific policies regarding the use of existing group mailing lists (e.g., all- students or all-faculty). Contact your campus IT organization for details regarding these policies.
7. Spoofing, or attempts to spoof or falsify email, network or other information used to identify the source, destination or other information about a communication, data or information is prohibited.
8. You must not degrade computing or network performance in any way that could prevent others from meeting their educational or College business goals.
9. You must conform to laws and Colleges policies regarding protection of intellectual property, including laws and policies regarding copyright, patents and trademarks. When the content and distribution of an electronic communication would exceed fair use as defined by the Federal Copyright Act of 1976, users of campus computing or networking resources shall secure appropriate permission to distribute protected material in any form, including text, photographic images, audio, video, graphic illustrations, and computer software.
10. You must not use campus computing or networking resources or personal computing resources accessed through campus network facilities to collect, store or distribute information or materials, or to participate in activities that are in violation of federal, state or local laws.
11. You must not use campus computing or networking resources or personal computing resources accessed through campus network facilities to collect, store or distribute information or materials in violation of other Colleges policies or guidelines. These include, but are not limited to, policies and guidelines regarding intellectual property and sexual or other forms of harassment.
12. You must not create or willfully disseminate computer viruses. You must employ appropriate virus protection methods to avoid damaging CNF resources.
13. Use of CNF resources for advertising, selling and soliciting is prohibited without the prior written consent of the Colleges, and use of CNF resources for commercial purposes or for personal financial gain is prohibited. Faculty, students or staff who have questions about the legitimacy of a particular use should discuss it with the appropriate members of the IT staff on their home campus.
14. The disclosure of individually identifiable non-directory information to non-university personnel is protected by the Family Educational Rights and Privacy Act of 1974 (FERPA). The disclosure of financial or personnel records that are owned by the Colleges without permission or to unauthorized persons is not permitted and may be prosecuted under California Penal Code 502.
15. Willful or unauthorized misuse or disclosure of information owned by the Colleges will also constitute just cause for disciplinary action, including dismissal from school and/ or termination of employment regardless of whether criminal or civil penalties are imposed. It is also expected that any user will report suspected abuses of CNF resources. Failure to do so may subject the individual to loss of CNF access and/or the disciplinary action referred to above.

The respective Information Technology organization of one of The Claremont Colleges may immediately suspend service to an individual or computer found to be significantly degrading the usability of the network or other computer systems. Inappropriate use will be referred to the appropriate College authority to take action, which may result in dismissal from school and/or termination of employment.

Password/Security Codes: Individuals entrusted with or that inadvertently discover logins and passwords are expected to guard them responsibly. These passwords are not to be shared with others. The same policy applies to door codes for restricted-access rooms/areas. Those who need logins or door codes can make a formal request to the administrator of those codes/passwords. **Note**: The provisions of this Policy apply to the institutions comprising The Claremont Colleges. (rev. 6/27/02)