D. The search of the entire premises must be conducted by Huntingdon College Security Personnel with assistance from Montgomery Police Officers and Montgomery Fire Department Personnel if necessary, in order to note anything alien to the surroundings.

E. If a suspicious object is located, DO NOT TOUCH IT! and DO NOT MOVE IT! Security Personnel and/or Montgomery Police Officers should be stationed at a safe distance to cordon off the danger zone, and the E.O.D. Unit will be contacted by a member of the Montgomery Police Department to respond to the scene if necessary.

F. After the search has been completed, the Montgomery Police Department will complete an incident report of the bomb threat. Remember that a bomb can be almost anything, ranging from the most overt bundle of explosives to cleverly concealed, ordinary objects. A briefcase, toolbox, and pieces of pipe could be used. You will be looking for something that doesn't belong. If anything appearing to be a bomb is to be found, DO NOT TOUCH IT! And DO NOT MOVE IT! The police will take charge and decide the course of action.

G. In the event of an actual explosion, then the primary command concerning fire control and injuries would be shifted to the Montgomery Fire Department. The Montgomery Police Department would then be primarily responsible for maintaining the scene, traffic control and any investigation that might follow. The Huntingdon College Emergency Plan would immediately go into effect.

APPENDIX VII
TECHNOLOGY
Computer Users' Privileges and Responsibilities for Huntingdon College Computing Resources

I. Introduction

This is the policy for the personal and public access computing resources at Huntingdon College. The policy reflects the ethical principles of the College community and indicates, in general terms, what privileges and responsibilities are characteristic of the College computing environment.

II. General Policies

Computer use is an essential part of many activities at Huntingdon College. The general policies regarding the resources provided by Huntingdon College are outlined below.

Access - Access to Huntingdon College computing resources will be provided to all members in good standing of the Huntingdon College community. There are no special fees for normal computer use.

Availability - Huntingdon College computing resources are available to users with as few interruptions as possible. Public access areas are generally open on a first-come, first-served, 24-hour-per-day, seven-day-a-week basis during the regular school year. Shorter hours may be in effect during holidays and summer terms.

III. Security and Censorship

Anyone who uses a computer should be aware that the information stored in it is inherently insecure and that shared computing facilities present security and confidentiality hazards that do not occur on a computer controlled solely by the user.

Censorship -- Free expression of ideas and free access to the ideas of others is central to the academic process. System administrators are not censors and will not remove, because of its content, any information from computers unless the administrator finds that: 1) The information involves illegality [e.g., material that violates copyright laws,

federal pornography laws, or licensing agreements], or, 2) The information endangers or impedes computing resources [e.g., a computer virus, worm, spyware or other destructive or intrusive program]. System administrators may remove any information defined above.

IV. Responsibilities of the User

Access to Huntingdon College computing resources is a privilege to which all Huntingdon College faculty, students, and staff are entitled, much like the privilege of using the resources of the Houghton Memorial Library. Certain responsibilities accompany this privilege; understanding them is important for all computer users. These responsibilities are described below.

Institutional Purposes -- Huntingdon College computer resources are provided for the support of College-related activities. Use for academic purposes (such as for the preparation of class assignments) is primary; other use (such as for campus organizations) is secondary. Reasonable personal use (e.g., for Internet surfing or game playing) is allowed provided it does not tie up resources needed for College-related work or unreasonably interfere with such work. Use for business purposes, for private gain, or for an activity unrelated to the College is prohibited.

Security and Confidentiality -- The user is responsible for correct and sufficient use of the tools provided by each computer system for maintaining the security and confidentiality of information stored on it. For example:
* The user is ultimately responsible for the security and confidentiality of information stored in their computers.
* Computer passwords are assigned to individual users and are not to be shared with others.
* The user must not reveal their password deliberately or inadvertently, and must change it if there is reason to believe it has been compromised.
* The user is responsible for understanding the level of protection each computer system automatically applies to files and must supplement it, if necessary, for information the user deems sensitive.
* The user must be aware of computer spyware, viruses and other destructive programs and must take all reasonable steps to avoid being their victim or unwitting vector.

Legal Usage -- Huntingdon College computing resources may not be used for illegal purposes including, but not limited to:
* Intentional or negligent destruction or damage to equipment, software, or data belonging to the College or to other users.
* Intentional or negligent disruption or unauthorized monitoring of electronic communications.
* Unauthorized downloading or copying of copyrighted material (e.g., using peer-to-peer software to download illegal copies of music, motion pictures or software).

Ethical Usage -- Computing resources must be used in accordance with the high ethical standards of the College community. Examples of unethical use follow; some of them may also be illegal.
* Unauthorized use or disclosure of computer access codes.
* Net abuse: intentional use of computer facilities in ways that unnecessarily impede the computing activities of others. This includes the unsolicited e-mailing of the same message to a large number of individuals (spamming).
* Using the computer facilities for private purposes or for personal profit.
* Academic dishonesty (plagiarism, cheating.)
* Violation of software license agreements.
* Violation of Huntingdon College computer usage policies and/or regulations.
* Violation of another user's privacy.

The ethical standards of Huntingdon College demand the practice of collegial computing including:
* Being sensitive to the public nature of computing facilities, even in the Residence Halls, and taking care not to deliberately display in such locations images, sounds, or messages which could create an atmosphere of discomfort or harassment for others.
* Refraining from intentionally transmitting to others at any location inappropriate images, sounds, or messages which might be reasonably considered harassing.
* Refraining from overuse of campus computer resources including printing facilities or network capacity.
* Respecting the rights of other users by avoiding disruptive behavior.

Information in electronic form must meet the same standards for distribution or display as if it was tangible. Users are free to publish their own opinions, but must not attempt to falsely attribute them to others. The creation, alteration, or deletion of any electronic information contained in, mailed to, or posted to, any computer or network will be considered forgery if it would be so considered on a tangible document or instrument.

V. Huntingdon College Peer-to-Peer File Sharing Policy

"Peer-to-peer" computer software allows the end user to download and share music, movies, images, software, video, etc., with other users running the same software anywhere on the Internet.

Because almost all of the content shared by "peer-to-peer" applications is in violation of the Digital Millennium Copyright Act (DMCA), and in most cases in violation of numerous copyright and Federal pornography laws, and because they are a violation of Huntingdon College policy by saturating and monopolizing campus network resources with illegal activity, these applications are prohibited on the Huntingdon College Internet network. This means that:

1. Peer-to-peer file sharing applications including, but not limited to, Kazaa, Kazaa Lite, IMesh, WinMX, and others, may not be installed or used on computers or any device connected to the Huntingdon College Internet network.
2. Huntingdon College Technology Support Services staff (the Tech Team) may, in order to ensure compliance with Huntingdon College policies and Federal and State law, require that the prohibited software be removed from any computer attached to the Huntingdon College Internet network, or that the computer be permanently disconnected from the network.
3. To perform their assigned duties, Huntingdon College Technology Support Services staff installs and maintains software on all student computers connected to the campus network that allows them to remotely troubleshoot all connected devices and ensure compliance with all Huntingdon College policies.

Violators of this policy will be subject to disciplinary action in accordance with current Huntingdon College disciplinary policies.

VI. Sanctions

Violations of the policies described in this document for legal and ethical use of computer facilities will be dealt with seriously. Violators will be subject to the normal disciplinary procedures of the College, which may result in, among other possible sanctions, suspension of Internet access or computing privileges.

VII. Acknowledgments

This document is modeled upon and portions are, with permission, taken from Computer Users' Privileges and Responsibilities, a publication of University Computing Services, Indiana University, Bloomington, copyright 1993 by the Trustees of Indiana University. Portions are adapted from 1992-1993 Guidelines for use of Campus and Network Computing Resources, Princeton University.

VIII. Campus Telephone Procedures

To connect your phone to the campus telephone system, plug your phone into the phone jack in your campus bedroom. If you don't get a dial tone contact the Tech Team in the basement of Flowers Hall. If you can't call an off-campus number or if your assigned campus phone number does not ring in your, call ext. 5678 and follow the verbal instructions.

If you move to another room on campus, you will need to get your assigned phone number moved to your new room. To do this, plug your phone into the phone jack in your new room and call ext. 5678 and follow the verbal instructions. Your assigned phone number will be moved to your new room as soon as your room change paperwork is complete and Residential Life gives the OK to move the number.

To call off campus, dial 9, then the seven-digit phone number. People calling your room should dial the campus prefix, 833, and your assigned four-digit number. Long distance service is charged at $ .10 per minute any time, anywhere in the country. You received a long distance authorization code when you registered. Safeguard it, because you are responsible for all long distance calls placed with your authorization code. To dial long distance, dial 9, then the long distance area code and the phone number. When you hear a beep, enter your authorization code and the call will then go through. You can make long distance calls from any dorm room and the calls will be billed to you. Outgoing 800/866/877/888 calls cost $ .10 per call.

IX. Campus Communication

Huntingdon College will contact you with official correspondence and information via your assigned campus phone number and voice mail box, your Huntingdon email address and your campus mail box in the Delchamps Mail Center. There are the official means of contacting students. If you wish to not use any of these services, you will miss valuable information but you will still be held responsible for it.