

OB\GYN DEPARTMENT ACCEPTABLE USE POLICY

The Acceptable Use Policy for the OB\GYN department comprises two parts:

1. [University of Florida AUP](#)
2. [Additional OB\GYN Policies](#)

UNIVERSITY OF FLORIDA ACCEPTABLE USE POLICY

All computers and computing resources used in the department are subject to the [University of Florida Acceptable Use Policy](#).

Among other things, this policy prohibits the use of departmental computers and computing resources for any of the following purposes:

- to commit libel
- to violate privacy laws
- to violate [copyrights](#) or [trademarks](#)
- to violate laws of obscenity and child pornography
- to violate the [Florida Computer Crimes Act](#)
- to violate the Electronic Communications Privacy Act
- to violate the [Computer Fraud and Abuse Act](#)
- to engage in hacking, cracking, or similar activities
- to violate the [Student Code of Conduct](#)
- to violate the [Sexual Harassment Policy](#)
- to gain unauthorized access to remote computers
- to impair or damage the operations of UF computing facilities
- to attempt to circumvent data protection or security measures

In addition, computer accounts may not be:

- shared between users (i.e. you may not share your password under any circumstances)
- used for commercial purposes, or for personal financial (or other) gain

Certain uses of email are prohibited including:

- chain mail
- harassing or hate-mail
- virus hoaxes
- spamming or e-mail bombing
- junk mail
- false identification

ADDITIONAL OB\GYN POLICIES

Currently, the OB\GYN department uses the [UF AUP](#) without modification. The following practices are also explicitly forbidden:

- Placing any non-OB\GYN administered computer on the OB\GYN managed network including personal machines and laptops.
- Computer accounts may not be shared in any way. This includes sharing your password, allowing others to use your account, or in any other way providing UF computing resources to any other person.
- Any attempts to compromise the security of OB\GYN computing facilities, steal passwords, launch denial of service attacks, or attempt to break into other computer systems will be grounds for immediate termination of the OB\GYN account.
- Practices commonly used to bypass security including cracking and/or guessing passwords, network sniffing, and scanning the network for vulnerabilities.
- User maintenance of OB\GYN managed machines is forbidden. This includes unhooking a computer from the network, attaching peripheral devices, opening it up, etc. ALL maintenance on OB\GYN managed equipment must be done by OB\GYN IT staff.
- Creating a home page which violates the OB\GYN Acceptable Use Policy.

I have read this policy and by signing below agree to abide by these terms and conditions.

Signature: _____

Date: _____