You may not deliberately attempt to disrupt the performance of a computer system or a network, on or off campus. You may not attempt to ‘break’ system security. You may not reconfigure computer systems to make them unusable for others. You may not attempt to destroy or alter data or programs belonging to other users. You may not modify residential computing network services or wiring or extend those beyond the area of their intended use. This applies to all network wiring, hardware, and cluster and in-room jacks. Gateways and firewalls designed for home use, such as Cable/DSL routers and wireless access points, can disrupt the normal operation of the Williams network and are not allowed. You are responsible for protecting your computer and not allowing others to use your computer to attack others on the network. Specifically this means that you are required to be running a *supported*, up-to-date, anti-virus package and to ensure that your computer has had all applicable security patches installed.

You may not copy or redistribute software or other information that is copyrighted. By US law, software piracy is a felony. You may not attempt to override copy protection on commercial software. The ability to find and read information on computer systems does not mean that the information is in the public domain. Having the ability to read does not necessarily grant the right to copy or redistribute. Nor, even, in the case of certain information on the Internet, does ability to read mean that permission to read has been lawfully g

Williams College has wr

Covid-1

li
lle

op