Title: College Network and Software Usage	Number: 6Hx2-8.01
Legal Authority: *Fla. Stat.: 119, 815, ~~1001~~10001.65*	**Page:** ~~1 of 3~~ 1 of 3

GENERAL STATEMENT

The President shall establish procedures as necessary to ensure proper, secure and efficient use of the Broward College (The College) Network and all software installed on equipment attached to the College Network. Installation of software will only be performed by authorized personnel, and then only if the software has been approved as compatible with the College Network and ownership of a valid license has been established. The College Network is intended for college and academic use only.

~~THE POLICY and THE STUDENT~~

~~The College provides all of its students with College Network and Internet access so that they can obtain up- to-date information useful for their advancement in academics. It is the student's responsibility to understand what constitutes proper use of the College Network, as outlined in Procedure B6Hx2-8.01 College Network and Software Usage by Students.~~

THE POLICY and THE FACULTY AND STAFF

The College provides all ~~of~~ its employees with ~~a~~ College Network and Internet access so that they can obtain up-to-date information useful to them for the performance of their job functions and duties. It is the employee's responsibility to understand what constitutes proper use of the College Network, as outlined in Procedure A6Hx2-8.~~01~~01a College Network and Software Usage by Employees.

THE POLICY and THE STUDENT

The College provides all of its students with College Network and Internet access so they can obtain up-to-date information useful for their advancement in academics. It is the student's responsibility to understand what constitutes proper use of the College Network, as outlined in Procedure A6Hx2-8.01b College Network and Software Usage by Students.

IMPLEMENTATION and OVERSIGHT

Information Technology Staff will ensure all devices connected to the College Network comply with college policy. User accounts are provisioned to use Multi-Factor Authentication (MFA) for accessing the College's Network. Depending on the sensitivity of information being accessed, multiple layers of MFA may be required. On an annual basis, or sooner if the need arises, all devices on the College Network will be reviewed for approved and properly licensed software. All software in violation of College policy will be removed from the College Network. Prior to inspecting all devices, the list of approved software will be reviewed and updated by Technology Staff. Pursuant to Florida Statute Chapter 815 – Computer Related Crimes, ~~T~~the College will, as necessary and appropriate, monitor network activities to and from any computer directly connected to the College Network, including Internet access, to detect unauthorized

History: *New Policy – 03/21/2008 Combines 6Hx2-8.01 College Network and Software Usage by Employees and 6Hx2-8.02 College Network and Software Usage by Students; revised November 14, 2012;*

~~**History:** *New Policy – 03/21/2008 Combines 6Hx2-8.01 College Network and Software Usage by Employees and 6Hx2-8.02 College Network and Software Usage by Students; revised November 14, 2012; revised February 26, 2013; revised February 25, 2020*~~

~~Approved by the Board of Trustees~~ ~~Date~~ ~~2/25/2020~~	~~President's Signature~~ ~~Date~~ ~~2/25/2020~~

Title: College Network and Software Usage	Number: 6Hx2-8.01
Legal Authority: *Fla. Stat.: 119, 815, ~~1001~~10001.65*	**Page:** ~~2 of 3~~ 2 of 3

activity or intrusion attempts, and for diagnostic purposes. Such activities may be archived and monitored at a future date. The College reserves the right to use web filtering, content filtering and geo-blocking to control internet access and apply other network restrictions as it deems necessary. The College reserves the right to refuse, by physical and non-physical means, the ability to connect ~~personal computing~~devices ~~equipment~~ to Broward College's infrastructure and/or limit the ability of users to transfer data to and from specific resources on the Broward College network. Information Technology will also engage in such action if it feels such ~~equipment is~~devices are being used in a way that puts Broward College systems, data, and users at risk. The Information Technology and ~~Human Resources department~~Talent and Culture departments have the right to investigate all incidents and will make the final determination as to whether specific network usage is in violation of College policy. Due to Florida's very broad public records law described in Florida Statute Chapter 119 – Public Records, most electronic information to or from College employees regarding College business are public records, available to the public and media upon request. Therefore, files stored on the College network may be subject to public disclosure. Broward College monitors, tracks and audits connectivity and usage of all devices to the ~~Broward~~ College Network. Users ~~should not~~ do not have a reasonable ~~have an~~ expectation of privacy in information stored on or transmitted through the College Network. ~~related to personal or college owned computing equipment when connected to or using Broward College's computing resources.~~

VIOLATION OF POLICY

Employees in violation of these established procedures and requirements may be subject to disciplinary action, up to and including termination. Students in violation of these established procedures and requirements may be subject to disciplinary action as outlined in the Student Handbook. All individuals in violation may face fines, fees for damages, civil or criminal penalties from the U.S. courts.

DEFINITIONS

~~Personal Computing equipment or device~~Devices - Includes Personally owned laptops, desktops, smartphones, tablets and any other device that has computing power and can join a wired or wireless network ~~of any kind.~~. The college restricts Personal ~~Computing equipment~~Devices to internet access only.

College Network - A college-wide computer wired and wireless network that can include, but is not limited to~~:~~ servers, printers, ~~personal~~ computers, network ~~routers/~~switches, UPS systems, faxes, multi-functional devices, projectors, podiums/teaching stations, telecommunication systems, video conferencing, application software and systems, wireless access points, cellular phones, tablets and network cabling.

Approved and properly licensed software - Software that is listed on the College ~~web site~~website as approved software and licensing is provided by a valid site or individual license.

History: *New Policy – 03/21/2008 Combines 6Hx2-8.01 College Network and Software Usage by Employees and 6Hx2-8.02 College Network and Software Usage by Students; revised November 14, 2012;*

~~**History:** *New Policy – 03/21/2008 Combines 6Hx2-8.01 College Network and Software Usage by Employees and 6Hx2-8.02 College Network and Software Usage by Students; revised November 14, 2012; revised February 26, 2013; revised February 25, 2020*~~

~~Approved by the Board of Trustees~~ ~~Date~~ ~~2/25/2020~~	~~President's Signature~~ ~~Date~~ ~~2/25/2020~~

Title: College Network and Software Usage	Number: 6Hx2-8.01
Legal Authority: *Fla. Stat.: 119, 815, ~~1001~~10001.65*	**Page:** ~~3 of 3~~ 3 of 3

Information Technology Staff – The Vice-President of Information Technology, the Information Technology Leadership team, and each of their respective staffs. ~~–~~ In addition, the College may use consulting and contracted services to augment the Information Technology Staff.

5. ~~-~~

~~Necessary and Appropriate – Circumstances that are deemed necessary and appropriate are:~~ College reserves the right to access employee and student information on the Broward College Network as follows:

1. When carrying out routine computer service tasks, Technology Staff or other members of College discover data which breaches college policy, or where the nature of the data suggests such a breach has occurred or will occur.
2. When the user has voluntarily made such information accessible to the public, as by posting to a listserv, blog, or webpage
~~1.~~3. When it reasonably appears necessary to do so to protect the integrity, security, or functionality of College or other computing resources or to protect the College from liability

~~2.~~4. Where formal complaints are received suggesting that the College Network is being used to store, transmit or transfer data which breaches college policy, the College's contractual obligation to third parties, Florida or Federal Law.
~~3.~~5. Where the College has been required, or requested by law enforcement, to monitor data as part of a criminal investigation.
6. Where there is other reasonable suspicion that users are storing, transmitting or transferring data which breaches college policy, the College's contractual obligation to third parties, Florida or Federal Law.
~~4.~~ 7. To aid in the investigation of a violation of law or college policy by an employee or student.

The College reserves the right to change this policy at any time without prior notice or consent.

History: *New Policy – 03/21/2008 Combines 6Hx2-8.01 College Network and Software Usage by Employees and 6Hx2-8.02 College Network and Software Usage by Students; revised November 14, 2012;*

~~**History:** *New Policy – 03/21/2008 Combines 6Hx2-8.01 College Network and Software Usage by Employees and 6Hx2-8.02 College Network and Software Usage by Students; revised November 14, 2012; revised February 26, 2013; revised February 25, 2020*~~

~~Approved by the Board of Trustees~~ ~~Date~~ ~~2/25/2020~~	~~President's Signature~~ ~~Date~~ ~~2/25/2020~~