

Richard Bland College Employee Computer Use Policy

I. Employee Use of Computers

Richard Bland College must be protected from potential loss due to careless, malicious, or unethical use of the College's personal computers. Employees will be governed by all official policies of the College, including the "Richard Bland College Computer Use Policy" as published in the Student Handbook, in the Faculty Handbook and on the Richard Bland College website. (<http://www.rbc.edu/>)

Employees are obligated to comply with all applicable laws, regulations, contracts, licenses, policies, standards, organizational controls, security rules, etc. In particular, the individual user is responsible for understanding and complying with all copyright laws.

RBC users of computers attached to the campus network have a common responsibility to fellow users to follow security policies designed to protect the campus network. This includes adhering to virus scan procedures, refraining from visiting risky web sites (such as game sites), following file download instructions and other security-based instructions issued by Information Technology Services and or listed on the IT area of the RBC web site. ([Restricted Sites](#))

Certain programs, such as Instant Messaging and file sharing programs, constitute a network security risk and may not be installed on computers connected to the RBC network. The ITS section of the RBC Intranet web site provides a current list of these programs. FTP and telnet protocols may be used only with specific approval of the IT staff. Other programs that consume significant resources or affect PC performance may also be prohibited on a case-by-case basis.

The following policies also apply to the use of Richard Bland College's personal computers by employees:

1. Personal computers and printers procured by the College are to be used for College purposes only. Use for College purposes includes:
 - a) instructional and administrative activities
 - b) activities that support personal development and education

- c) activities that support community service
 - d) limited personal use, as long as it does not interfere with the proper use of the PC for normal duties, violate college policies or laws or place an undue burden on network resources
- 2. Under no circumstances may employees use their personal computer for commercial purposes.
- 3. The off-premises use of personal computers to access the College's communications network, computers, data files, or programs is governed by the same policies as on-campus use.
- 4. Certain devices, such as laptops, jump drives, portable projectors and cameras, are by their nature mobile. Employees to whom mobile devices are issued assume a special responsibility to guard them against theft, loss or damage. When a laptop or other portable equipment valued over \$500 is assigned to an employee, the employee must sign a responsibility statement prior to issue and yearly thereafter.
- 5. Removal of other personal computer hardware and/or software for off-premises use may be permitted for a limited period. Both of the following conditions must be met:
 - a) Prior written approval has been given by the applicable dean (Dean of Administration and Finance or the Provost).
 - b) The user has signed a statement of responsibility for the equipment and/or software.
- 6. Personal-computer users performing administrative functions are responsible for the integrity and security of the data used, including:
 - a) Correctness of results.
 - b) Correctness of any associated data base(s) (including the use of appropriate controls and audit trails, detection of variances, and exercise of any necessary College action).
 - c) Procedural documentation and proper labeling of reports (including authorization, date of preparation, identification of data and its source).
 - d) compliance with laws and regulations designed to protect privacy and security of data, such as the Family Educational Rights and Privacy Act (FERPA) and those which safeguard Personally Identifiable Information (Pii).

7. Formal back-up procedures must be established and adhered to at all times to prevent loss of data.
8. Every employee shall be given a copy of these policies and he/she shall sign a written statement that he/she understands and agrees to comply with these policies.
9. In case of emergency requiring exceptions to these policies for any reason, requests should be made to the Dean of Administration and Finance.

II. PC Hardware and Software Acquisitions

The College has developed standards for the brands and models of hardware and software that it will purchase. To ensure they conform to these standards, the Director of Information Technology Services will review all faculty and administrative computer hardware purchases. The Director of Information Technology Services will review all administrative employee software purchases. Faculty should seek the advice of the Director of Information Technology Services before purchasing additional software not covered by the MS Campus Agreement.

III. General Care and Maintenance of Personal-Computing Hardware

The personal-computing environment shall not cause the equipment to be exposed to adverse/hazardous conditions. The following policies shall be followed:

1. Proper temperature and humidity levels shall be maintained, as recommended by the equipment manufacturer.
2. Equipment shall be protected from pollution, dust, and other contaminants:
 - a) Smoking will be prohibited in areas where the equipment is operated and/or files are stored.
 - b) Equipment will be cleaned periodically, as prescribed by the manufacturer.
 - c) Food and/or beverages will be prohibited/restricted in the work areas.
3. Equipment shall be reasonably protected from fire, water, power hazards, and static electricity.
 - a) All electrical equipment will be properly grounded.

- b) Surge-protectors or surge-arrestors will be used. All PCs will be protected by UPS battery backups or integral laptop batteries.
 - c) Computer hardware, software and data diskettes will be kept at least 5 feet away from all magnetic and/or electrical devices.
4. During electrical storms, power outages or brownouts, normal shutdown procedures should be followed, and then the computer should be turned off. **Never turn off the UPS, unless instructed to do so by ITS.**
 5. Only **authorized** individuals will perform equipment maintenance or modification. This authorization must be given by the Director of Instructional Technology for academic lab computer equipment, or by a member of the Information Technology Services staff for all other equipment.
 6. Equipment handling and moving shall be done in accord with the manufacturer's instructions and by **authorized** individuals only. This authorization must be given by the Director of Instructional Technology for academic lab computer equipment, or by a member of the Information Technology Services staff for all other equipment.
 7. Employees are responsible for reading operational manuals for their PCs, monitors, printers and similar technology tools and to follow the manufacturer's recommendations for use.

IV. Grant and Removal of Employee Access to Technology Resources

1. No access will be granted without submission of an Richard Bland College Employee Security Access Checklist form. This form must be completed by the employee's supervisor. Additional authorization is required to initiate and specify access to eVA and the Banner Enterprise Resource System.
2. To obtain an RBC email account, the employee must also fill in a form requesting access and promising to adhere to published college technology policies and guidelines for use, and they must complete security training.
3. The Provost's Office will notify ITS each semester which adjunct faculty will be teaching, and will see that the new and rehired adjuncts fill in the email account application. The HR department will notify ITS at the beginning of each semester

which student workers will be employed for that semester so that their paperwork and security training can be completed.

4. The Human Resources Department is responsible for notifying the Institutional Security Officer (ISO) when employees are hired, terminated or change positions, prior to the effective date of such changes. Supervisors are responsible for updating the Employee Security Access Checklist and submitting it to the ISO prior to the effective date of employment changes or whenever access is first needed.
5. Requests for access to eVA must be approved by the Dean of Administration and Finance.
6. Each functional area (Student, Finance, Financial Aid) has a designated Banner Security Coordinator who is the only person who can authorize changes to internal Banner security access (forms, processes, etc.). These change requests must be submitted in writing to the IT Banner Security Officer. When changes are applied, the IT Banner Security Officer will provide printouts of the current security access granted to all employees of their respective areas to the functional Banner Security Coordinator.
7. The Banner Security Coordinator is responsible for requesting the removal of access that is no longer appropriate due to changes in functional duties or employee termination at the time when the change of duties occurs. This responsibility does not relieve the employee's supervisor of the duty to notify the Banner Security Coordinator 3-5 days before such change in duties occurs.
8. Any extension of access to employees who have changed duties must be made in writing and will only be granted for a specified period of time based on demonstrated need. The Banner Security Coordinator for each area will review access on a semi-annual basis to ensure that obsolete access grants have been removed.

V. State Laws Regarding Use of Computer to Access Materials with Sexually-Explicit Content and Other Constraints on Use of the Internet and Electronic Communications Systems

This Policy recognizes the existence of state laws governing access to materials with sexually-explicit content. Prohibited activities include accessing, downloading, printing or storing information with sexually

explicit content as prohibited by law (see Code of Virginia §2.1-804-805; §2.2-2827 as of October 1, 2001).

Users are encouraged to read and abide by the full Department of Human Resource Management (DHRM) Policy Number 1.75-Use of the Internet and Electronic Communications Systems on the DHRM web site: http://www.dhrm.state.va.us/hrpolicy/web/pol1_75.html.

VI. Penalties

Employees who violate the computer use policies of the college will be issued a verbal or written warning. Employees who willfully disregard the warning will be subject to termination of computer network access or removal of the college computer from their office, as appropriate. This action will be recommended by the Director of Information Technology Services but must be approved by the Dean of Administration and Finance and the Provost. Employees will be notified in writing and copies will be placed in their personnel file.