STATE OF NEW JERSEY
DEPARTMENT OF CORRECTIONS

TO: Inmate Population DATE: 10/9/90

FROM: Patrick Arvonio, Administrator

SUBJECT: Procedures for the Purchase of Personal Microcomputers

The purpose of this memo is to update institutional policies and procedures with regard to the above noted equipment.

Effective immediately, word processors, electronic typewriters, and personal computers are considered permissible personal property which can be acquired by individual inmates and sanctioned inmate organizations.

1. Definition:

   A microcomputer is a computer system whose processing unit is a microprocessor (an integrated circuit that accepts coded instructions for execution, which allows the machine to be programmable), and includes storage and an input/output facility in addition to the microprocessor.

2. Possession of microcomputers, software, and peripherals by inmates and inmate organizations is a privilege, not a right.

3. All computer equipment, supplies, and peripherals must be obtained from an appropriate source of sale.

4. Each inmate and/or inmate organization may be permitted to own one stand-alone microcomputer, which must be attached to a surge suppressor which can have a maximum of 4 plugs with a power cord no longer than 6 feet. The total cost of the microcomputer and all peripherals including the printer cannot exceed two thousand dollars.

5. The microcomputer may be attached to one non-letter quality, dot matrix printer.

6. All computer equipment and peripherals owned by an individual may only be located in that individual's cell or immediate bed area.

7. All such equipment and peripherals owned by an organization must be located in that organization's office or approved work area.

8. Inmate and inmate organizations owned microcomputers may not be connected to a modem, any other computer system, or network.

9. Internal and external modems are prohibited.

10. Peripherals permitted are:

a. Video monitor-screen size to be no larger than 14" diagonally.

b. No more than two (2) disk drives.

c. One non-letter quality dot matrix printer.

d. One (1) surge suppressor.

e. One (1) 6 foot, 4 plug outlet adapter.

11. Peripherals prohibited are:

a. Maintenance items.

b. Cleaning supplies.

c. Analog to digital connector.

d. Internal and external modems.

12. An Institutional staff member has been designated as the Institutional Computer Security Manager. All requests to purchase and possess microcomputer hardware and peripherals are subject to review procedures developed by the Computer Security Manager.

13. Computer equipment which requires service shall be returned directly to a factory authorized service center at the inmate's or organization's expense.

14. A microcomputer owned by an individual inmate is for the personal use of the inmate owner only.

15. Computer equipment owned by an inmate organization may be used for the activities of that organization only.

16. The use, programming, or storing of any inmate or inmate organization owned equipment for institutional or departmental staff is prohibited.

17. Neither the institution or the Department of Corrections will be responsible or liable for damage to the personal computer or data stored within it as a result of power outages, electric power surges, institutional disturbances, or inmate theft or vandalism.

18. Education Department computers may not be connected to any other computer system, or modems. Educational local area networks (LANS) are permitted but must be confined to a

classroom or school area, and may not be connected to a modem. Any LANS can only be used for instructional purposes. Any computerized educational application which requires a modem must be approved by the Deputy Director of the Division of Policy and Planning prior to purchasing and installation.

19. Inmate access to an Institutional or Departmental computer or computer system is prohibited, as is access to any system using or maintaining institutional or departmental data.

20. Computer systems applications developed by inmates or inmate organizations and used by institutional staff must be discontinued and purged. Inmates and inmate organizations may not develop such applications.

21. In order to obtain permission to obtain as a gift or purchase computer equipment, peripherals, or software, the attached "Computer Purchase Authorization Form" must be filed with the Computer Security Manager.

22. When the request is approved, all appropriate parties will be notified by the Computer Security Manager.

23. Any equipment ordered and received by the institution prior to approval will be confiscated and returned to the vendor at the inmate's or organization's expense.

24. The Computer Security Manager will determine the appropriateness of software requested by any inmate and will not permit its acquisition in the event the software is considered detrimental to the security and stability of the institution.

25. The following types of software will be prohibited:

a. All communications software including "office manager" and similar packages which contain communications programs.

b. Encryption or encoding programs.

c. Architectural design or floor plan software.

d. Forms Design software.

e. Gambling software or programs.

f. Local Area Network (LAN) or Wide Area Network (WAN) software.

26. Once permission is granted to purchase a computer, or obtain a computer as a gift, upon its receipt, the inmate and all current inmate officers of an organization must read and sign the attached "Computer Waiver Form". The Mailroom

Sergeant will secure the appropriate signatures and will distribute the copies accordingly. Staff liaisons of the organizations will work with the Mailroom Sergeant to ensure each inmate officer of the organization has completed the form.

27. Failure of all current inmate organization officers to fill out the Waiver Form will result in the group losing its privilege to possess the equipment.

28. As inmate officers of organizations change, newly installed officers must sign the waiver. Staff liaisons of the organizations will be responsible for informing the Computer Security Manager of changes in organizational staffing.

29. All inmate and inmate organization owned computer equipment is subject to periodic searches. All data stored within the equipment is subject to similar scrutiny.

30. Duplicating copyrighted software is a violation of copyright law and is prohibited.

31. Copyrighted software may only be obtained through direct purchase from an institutionally approved source of sale.

32. Backup of inmate owned computer data is the sole responsibility of the individual or organization involved.

33. The Computer Security Manager will maintain an inventory of inmate and inmate organization owned computer equipment on the System 36 using the Fixed Assests application program.

34. Violation of this policy may result in disciplinary action and termination of computer privileges, if applicable.

35. All inmates and inmate organizations who currently possess a personal computer which may be valued in excess of $2,000 are permitted to retain this equipment without being in violation of this procedure.