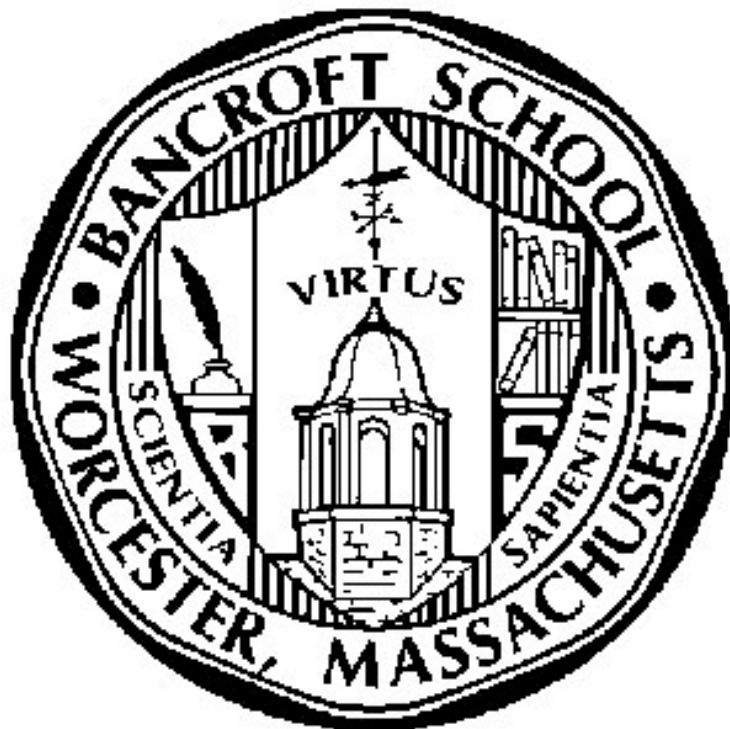


Bancroft School



Technology Policies and Procedures

Academic Year 2005-2006

Revised February 27th 2006

Table of Contents

Technology Mission Statement Definition of Technology for Bancroft School	page 2
Policies Connecting to the Bancroft Network Network and Internet Access Remote Access Software E-mail Technology Lab Use Scheduling and Borrowing Technology Equipment Laptop Cart Care and Use Laptop Loaners Employee Technology Purchases On-Campus Repair and Support Weekend and Vacation Support Home Repair and Support Device/Media Disposal and Re-use Non-Disclosure and Confidentiality Agreement Passwords Back-up	page 3 - 7
Procedures Documentation Back-up Disaster Recovery Network Security Account Creation User Name Creation Passwords Termination of Access Student School Migration Updates/Upgrades Server Replacement Cycle Desktop Replacement Cycle Laptop Replacement Cycle Faculty Laptops Desktop Use and Security Application and New Product Roll Out New Project Process Adding New Features/Reports to Existing School-Wide Data Bases Support/repair Procedures Technology Department Fail-Over Coverage Donated Hardware	page 8 – 13
Disclaimer	page 14

Bancroft School Technology

Mission Statement

Bancroft School's Technology Department strives to provide leadership, development, and support for both emerging and existing technologies to support the mission of the School.

We foster an academic culture that explores and values technology as an essential learning resource.

We expand our students' knowledge and assist them with adopting technology in academically meaningful and effective ways.

We support new technologies to enhance traditional instruction and the teaching and learning process.

We develop, establish and maintain systems and procedures that ensure an industry standard operation.

We also believe that technology needs to be a K-12 curriculum strand of knowledge and practical skills.

*Bancroft School broadly defines **technology** as the materials and processes that support and broaden the teaching, learning, assessment, and administrative functions of its students, faculty, and staff.*

*Bancroft School broadly defines **educational** as that which deals mainly with the methods and process of teaching and learning.*

Bancroft School Technology

Policies

Connecting to the Bancroft Network

The Bancroft's Technology Department, or commonly referred to as, "the Tech Department," maintains and operates the Bancroft School's computer system and network, collectively known as, "the network" or "the school's network," exclusive of the Business Office.

Only computers, peripherals, and other technology related devices, purchased, owned, operated and supported by the Tech Department are authorized to connect to the network. Devices include, but are not limited to, the following: desktop computers, laptops, printers, wired or wireless (Wi-Fi) hubs, switches, and routers, personal organizers (PIMs, Palm, etc.), digital music players (iPods, RIO, etc.), digital still and video cameras, USB flash keys, and scanners. All other devices are not authorized to connect to the network.

Only Bancroft School students, employees, authorized vendors and guests may connect to the network. Under special circumstances, and with prior written, or verbal permission from a Tech Department staff member, a device that is not owned or supported by Bancroft School may be allowed on the network. All devices will be inspected, and evaluated for compatibility, functionality, and security. Moreover, unless students have received prior authorization from the Tech Department, they are not allowed to connect any personal devices, other than USB flash keys, to the network.

Please Note: Access to the network is a privilege that can be revoked at anytime without notice.

Network and Internet Access

In order to gain access to the network and Internet, students and employees must read and sign an Acceptable Use Policy (AUP) at the beginning of each academic year. AUP's are available at the following locations: Human Resource office, Technology Department office, in the Employee Handbook, and on the Bancroft School website at <http://www.bancroftschool.org>.

Remote Access

Due to security concerns, remote access to personal files/accounts is not available at this time.

Software

All computers on campus are preconfigured or imaged with most of the software that is used on campus. Only members of the Tech Department staff are allowed to add to the school's base image; imaging occurs during summer and winter breaks. Requests to add software to the image must be received before these times.

Software that can be installed on an individual basis on Staff machines will be done as time allows. Such software must be school related, meaning no software will be installed for personal use (messaging, tax preparation, games, etc.)

E-mail

Bancroft School provides each employee with an e-mail account on an as-needed basis; E-mail can be accessed either through an e-mail client or a web browser.

Bancroft School's e-mail is not encrypted, so any critical information (passwords, etc.) **should not** be sent via e-mail.

This e-mail system should not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin, etc. Employees who receive e-mail with this content should report the matter to their supervisor immediately.

A reasonable amount of personal e-mail is acceptable, but users should save non-work related e-mail in a separate folder from their work related e-mail. Account users should not send chain letters because this activity quickly fills a user's account.

A member of Bancroft's Technology Department all virus or other mail-ware warnings needs will send to approve and mass mailings from Bancroft School before they are sent.

Bancroft employees shall have no expectation of privacy in anything they store, send, or receive on the school's e-mail system. Bancroft School may monitor messages without prior notice, but is not obliged to monitor e-mail messages.

Bancroft School treats its e-mail policy very seriously. If any employee violates the school's e-mail policy, the employee will be subject to disciplinary action, up to and including termination of employment.

Lab Use

Computer labs are located in the McDonough Center and the Stoddard Building. Teachers may sign up for lab use on the calendars or online database located in each lab or on the FileMaker server. Sign up is on a first-come, first-serve basis. Pre-assigned classes for lab use have priority over other students using the lab. Students using the computer labs will conform to the following rules:

- **Food and Drink** – Absolutely no food or drink is allowed in the lab. Anyone with food or drink will be asked to leave the lab.
- **Music** – Students may only play music on lab computers from compact disks and must wear headphones when listening to music. Unless they have been instructed by a faculty member to do otherwise, students may not copy or download music files to their Bancroft account.
- **Games** – unless a faculty member has given students permission, no game playing is allowed in the computer labs.
- **E-mail and Chats** - Unless they have been instructed by a faculty member to do otherwise, LS and MS students may not check their personal e-mail. No student is allowed to use the lab computers for chats or instant messaging.

- **Priority** – Priorities for use of lab computers are as follows:
 1. Regular classes meeting in the computer labs.
 2. Classes signed-up by teachers on the lab schedule.
 3. Working on homework and class projects during study periods, flex, and x-block.

- **Equipment** – Respect lab equipment. Do not remove or disconnect any labels, parts, or cables. Do not move computers. Do not change system settings, fonts, and desktop images.

- **Logging in** – Users are required to log into Bancroft computer lab machines and systems with their own unique username and password. No one should use another person’s username and password to gain access to the network. No one should give his or her information to another user. Anyone using another persons’ username password will be subjected to disciplinary action and/or suspension of his or her computer network privileges.

- **Logging out** – Even if only for a short time, all users should log-out of the system when they leave the computer labs. Failure to follow the log out procedure will cause a security breach on your account; anyone will be able to access your account without your knowledge.

Scheduling and Borrowing Technology Equipment

Technology equipment can be scheduled and borrowed by visiting one of the Technology Offices. The borrower must sign out each piece of equipment before they can take away any technology equipment. Only an employee of Bancroft School can borrow technology equipment valued at more than \$800.00. Borrowers are responsible for the equipment and must return the equipment in person; they cannot transfer the responsibility to another employee or student.

In order for technology equipment to be available for others, borrowed equipment must be returned as soon as possible after it has been used. If the borrowed equipment is not functioning properly, then it is the responsibility of the borrower to report the issue, as soon as possible, to a member of the Technology Department.

Students **are not allowed** take any technology equipment off campus.

Laptop Cart Care and Use

It is the teacher’s responsibility to transport a laptop cart to and from his/her area of use. At the end of each teaching session, laptops must be completely shutdown, returned into the cart, and plugged into the charging system. As a courtesy to other teachers, the cart should be returned to the Tech Storage location after each teaching session. Students **are not** allowed to move the laptop carts.

When a student logs into a laptop, he/she should use the username = bancroft and password = bulldog. If he/she has work to save, they should navigate over the network to save to their home folder or save their work to a flash drive. Any files that are saved to the laptop hard drive are not backed-up.

Laptop Loaners

The Tech Department has a few laptop computers available for employees to borrow either for class projects, or for short-term off-campus work purposes. When a laptop is taken off-campus, the local account should be used; all data stored on the laptop is the responsibility of the borrower. The borrower must sign a Laptop Loaner agreement before taking the laptop off-campus. The agreement specifies terms and conditions of use: time allotted, breakage penalty, etc.

Employee Technology Purchases

As a benefit, Bancroft allows employees to purchase computers through a no interest school loan. Payment and payroll deduction information should be discussed with the Director of Technology and the Business Office.

Bancroft School and its Tech Department **does not support or assume** any responsibility for technology equipment purchased by an employee for personal and non-institutional purposes.

On-Campus Technology Repair/Support

For repair and/or support requests, call extension either 611 or use the "Report a Problem" link on TechWeb website <<http://techweb.bancroftschool.org>>. All requests will be answered in a timely fashion. Mission critical issues will take priority.

Weekend and Vacation Technology Repair/Support

During vacation time, at least one member of the Technology Department will be on campus between the hours of 8:00 a.m. to 3:00 p.m. for each official school day.

During weekends and vacation breaks, our school network and computers are available for any employee's use. If an employee discovers a school-wide network and/or a multiple computer issue, then the employee should report the problem to extension 611 and leave a detailed.

Home Repair/Support

Personal home computers, printers, monitors, etc. are the responsibility of the owner. Members of the Tech Department are not expected to repair or update any of the student and/or employee's computers. For home repair issues, we recommend that they contact an authorized Apple Service Provider <<http://www.apple.com/contact/>>.

Although Bancroft School neither endorses, nor guarantees the workmanship or expertise of any particular vendor, Elkco at (508) 842-2111 is a vendor we use. The Tech Department also maintains a list of Bancroft School graduates who provide independent technology consultation services.

Device/Media Disposal and Reuse

Computer equipment can contain materials that are dangerous to the environment when broken or taken apart; therefore, all school owned computers, monitors, and printers that could possibly contain hazardous material are placed off the US Faculty Room in the back hallway until the recycling vendor is called to dispose of these items. Before equipment is dropped off their storage media (zip disks, hard drives, etc.) are erased and/or destroyed for security and confidentiality reasons.

Non-Disclosure and Confidentiality Agreement

Any unique or proprietary information (blueprints, bid documents, configurations etc.) that an employee of Bancroft School wants to share with an outside vendor, consultant, contractor, etc. requires a signed confidentiality agreement between Bancroft School and the recipient. For all intents and purposes, our standard confidentiality agreement should be acceptable for any vendor(s) to receive confidential information from the school.

Bancroft employees should only need to complete three fields on this document: recipient, name, and title. The confidentiality agreement document is password protected and located on the server listed below. If the confidentiality agreement needs to be modified, the user should contact the Technology Department to unlock and make changes to the document. This form can be found in the Forms folder on ADMIN-SHARE.

Passwords

Passwords are **not** to be shared; this will help prevent unauthorized access to mission critical information. When a user suspects that his or her password has been compromised, he/she should immediately contact the Technology Department to have all his/her passwords changed.

Back-up

Faculty/Staff/Student data files are backed-up daily. Copies of these files are moved offsite weekly.

iPASS™ data is backed-up to tape every night and stored off-site each day.

Alumni 4D back-up is done every week and saved to a CD and stored off-site by a member of the Development Office.

Bancroft School Technology Procedures

Documentation

All documentation for server and client services will be in the form of a "cookbook" or Operations Manual. The digital Operations Manual is located on the zeus.bancroftschool.org server, which can only be accessed by the Tech Department.

A hard copy of the Operations Manual is accessible during working hours and is stored during off hours in a locked file cabinet in the Tech Office. This documentation will allow the Technology Department to rebuild any server or service from beginning to end.

Backup

Faculty and student files/data reside on a redundant array of independent disks, or commonly known as a RAID. The RAID is comprised of the fourteen hot swappable hard drives and is capable of holding 5.4 terabytes of data. Seven drives are reserved for faculty / staff, while the remaining seven drives are reserved for the student body. A RAID 5 stripe configuration has been applied onto twelve drives. The remaining two hard drives are used for fail-over and redundancy.

Socrates (the faculty server) and Lyceum (the student file server) are connected to the RAID. Both servers use a Retrospect® client for nightly incremental backups. Retrospect® is owned by Datz / EMC Corporation and is widely used as a standard backup program for both Mac and Window operating systems. Every night, one automatic script instructs Retrospect® to backup the faculty RAID at 10:00 p.m., while another script is set to backup the student RAID at 11:59 p.m. If the faculty RAID has not the completed its backup procedure, then the student backup will wait until the previous task has been completed.

Hercules, the backup server, is responsible for controlling all of the Retrospect® data and scripts. Its three hard drives have been configured with a RAID 0 stripe configuration. All of the Retrospect® data is stored onto these three hard. Once a week, a second set of the Retrospect® data is copied onto a portable FireWire™ hard drive. Before moving the data off-site, the Directory of Technology, and/or the Network Server Administrator will test and review the data for integrity and ease of data recovery. This disaster recovery data is physically located in the Administration Building's storage closet and placed in a locked fireproof filing cabinet.

The iPASS™ backup consists of twenty 4mm tapes rotated on a daily basis from Monday to Friday. The tapes are divided into four groups of five in order to represent a month's worth of data backup; tapes are labeled Monday week 1, Tuesday week 1 etc. The magnetic heads on the iPASS™ server's backup tape module are cleaned once a week.

At the beginning of each workday, a tape from the appropriate week's rotation will be inserted into the iPASS™ database server. The automatic backup script is scheduled for 12:01 a.m. every morning and requires a tape to be already set in place. The iPASS™ backup tapes from the previous day are stored in the Administration Building's Storage Closet along with the portable FireWire™ hard drives. The Director or Network Administrator will take a two-day old iPASS™ backup tape off-site each night.

Disaster Recovery

In case of a disaster, the client's source data can be re-constituted from either the source data backups (one week old), or from the disaster recovery FireWire™ drives (two weeks old). At this time, no provision is available for the recovery of any data less than one week old. Future plans for either a SAN and/or RAID are being discussed. iPASS™ data backups should be able to be re-constituted from any one of the twenty 4mm tapes.

At this time, the source data, including FileMaker databases, have been tested for integrity and recoverability. Our iPASS™ data was tested and certified by IMG Software the weekend of October 22, 2005 as being fully able to be replicated from our 4mm backup tapes.

Network Security Incident

Firewall logs are reviewed every day. Any intrusion should be reported immediately to the offender's ISP via email; a stern warning template has been made. Each member of the department gets a copy of the abuse e-mail.

Account Creation

When a new employee joins our community, as a full time employee, or long-term substitute, or an employee of the Special Programs, the Account Creation Form on TechWeb needs to be completed. Depending on his/her needs, some or all of the following accounts will be created, network login access, e-mail, access to iPASS™, etc. When the Technology Department receives this form, the account(s) will be activated within 24 hours.

A member of the Technology Department, Division Head, Head of Special Programs, or his/her designee will meet with the new employee to ensure that they have access and understand how to use Bancroft School's technology.

When a new student joins our community during the school year, the respective Division Head, or their designee will complete the form on TechWeb. When the Technology Department receives this information, the student account will be activated within 24 hours.

The bulk information about students enrolled during the summer, are forwarded to the Technology Department by the Admission Department.

User Name Creation

Individual user names consist of the first letter of their first name and all the letters of the surname name. In case two users have the same user name, the youngest or newest user has their user name created by combining the first two letters of their first name and all the letters of the surname name.

Passwords

User Passwords are six characters long; four alphanumeric and two numeric. They are randomly generated. Initially, for ease of use, each individual user has the same password for all their accounts (login, e-mail, and database).

Students in grades 1-5 are given a password that is their grade number (students in grade 1 all have the password one). Students in grade 6 – 12 are given a unique six-digit password as described above.

Unique user passwords for employees are to be changed by the Tech Department every two years starting September 2005.

Server and network passwords are changed yearly.

Termination of Access

All accounts for members of our community who leave voluntarily will be deactivated the last day they are on campus, unless special arrangements have been made through the Administration and submitted to the Technology Department in writing. Before accounts are de-activated, the Technology Department will back-up their files to a CD.

All accounts (Login, iPASS™, e-mail, Curriculum Mapping, etc.) for members of our community whose employment/enrollment is terminated will be have their passwords changed immediately upon the Technology Department receiving written confirmation of their termination. Before accounts are deleted, the Technology Department will back-up their files to a CD. This CD will be given to the Headmaster. A copy will be kept in a secure area by the Technology Department for 6 months.

Student School Migration

When a student progresses from Lower School to Middle School and Middle School to Upper School his/her data will be removed from their account and backed-up to a CD. The CD's will be kept by the Technology Department and distributed to the owner once they have signed for it.

Updates/Upgrades

Most software and hardware updates/upgrades and migrations will be handled during the summer months or over a major vacation during the school year. They will be planned and tested ahead of time. Ample notification will be given to inform the community of this event via Tech Web and e-mail.

Server Replacement Cycle

The replacement of the servers is based upon the maximum life of the Apple Care extended warranty policy. At present, the AppleCare™ policy for servers is three years, thus the department will replace each mission-critical server every three years.

Desktop Replacement Cycle

Desktop computer upgrades, will occur every five years. Older computers are used in locations of limited use (LS/MS classroom student computers, etc.).

Laptop Replacement Cycle

Student laptops will be upgraded every four-years. It is the responsibility of the adult who is supervising student use of these laptops to inspect the laptop before and after it is used for damaged screens, and broken keys. It is also their responsibility to verify that the laptop is off before the lid is closed and that it is plugged back into a charger to ensure they will be in working condition for the next user.

Faculty/Staff members who would prefer to use a laptop instead of a desktop computer will be required to pay the difference in the cost between a new desktop unit and the laptop they have requested. They may elect to have this difference deducted from their salary interest-free over a 12-month period. Bancroft School will provide hardware and software support during this four-year cycle, and at the end of each four-year cycle, the faculty/staff member will own the laptop and be responsible for any and all future maintenance. If the faculty/staff member were to leave Bancroft before the end of a four-year cycle a pro-rated buyout will be established.

Faculty Laptops

A faculty member, whose primary computer is a laptop, will fill out a questionnaire before their laptop is set-up for them. A customized laptop configuration will then be created. User accounts for other family members, who might from time-to-time use this school laptop, will be set up by the Tech Department before the computer is distributed. Users of faculty laptops will also sign a Laptop Loaner agreement.

All laptops will have their operating systems and applications software updated as needed. It is the responsibility of the end-user to back-up his/her own data and schedule a time to have the laptop updated. The Bancroft Technology Dept. will back-up Faculty Laptops when requested.

Desktop Use, and Security

Access to desktop computers is available to all students and faculty. Since we use network home directories, any member of our community can log into their account and access their stored files/data from any computer on campus. No data is to be stored locally on the hard drives. All desktop computers are either in labs, classrooms, or in faculty work areas.

Student laptops are stored in locked metal laptop carts. Teachers who use these laptop carts must ensure that these carts are locked -- even when the laptop carts are not under their direct supervision. Faculty laptops are to be locked to their desks, when the laptop is not in their direct supervision. Laptops in the Library are to be in their locked cabinet when not in the direct supervision of the Librarian or the library staff. The Technology Department has a few additional laptops that are stored in their locked offices.

Application and New Product Roll Out

New applications or new versions of our current applications will be tested in the following manner. They will be tested for a minimum of two weeks by:

1. The Technology Department,
2. A small test group of mixed users
3. A larger cohort group before the application becomes part of the software image.

New Project Process

Usually new projects are born out of necessity, so the primary process should be based upon need and solving a need. A short process list should include the following:

- Initial equipment request
- Initial schedule - deployment and training
- Design for growth and flexibility
 - Expected growth
 - Growth schedule
- Budget, initial and long term (Total Cost of Ownership)
- Infrastructure restrictions over time
- Compatibility with existing systems

Adding a New Feature/Report to Existing School-Wide Databases

Data Base feature requests will be gathered and submitted in writing to the Technology Department by June 1st of each year. Requests will be discussed, approved, and prioritized by the Tech Department and Administrative Cabinet; every attempt will be made to have approved requests ready for September of that year.

Features that are deemed critical and are needed immediately by the Administration will require a funding mechanism.

Support/Repair Procedures

All calls to extension 611 and Tech Web reports are logged for future reference.

Items under warranty, after an initial review by a member of the Technology Department, are sent out for repair.

Items **not** under warranty will be serviced by the Tech Department first. If the item cannot be fixed by the Tech Department, then it will be sent to an outside vendor for servicing. The item will only be repaired if it is economically feasible and cost effective.

Donated Hardware

Recipients of hardware donated by Bancroft to them, are requested to send a thank you note itemizing the hardware received to the Headmaster and Director of Technology at Bancroft School.

Neither Bancroft School, nor its personnel assume any responsibility for supporting hardware that Bancroft has donated to a third party.

The Development Office will acknowledge in writing all hardware donated to Bancroft.

Dept. Fail-Over Coverage

When the Director of Technology is not on campus, the Instructional Technologist will cover the iPASS™ and training issues. The Network Administrator and Support Engineer will share the administrative and web issues.

When Network Administrator is not on campus, Director of Technology and Support Engineer will cover his network and server issues.

When Support Engineer is not on campus, Director of Technology and Network Administrator will cover his support calls.

When Instructional Technologist is not on campus, Director of Technology and Support Engineer will cover her responsibilities.

Disclaimer

1. The Technology Department at Bancroft School reserves the right to make changes to these policies and procedures in the future, without advance notice.
2. Bancroft School reserves the right to run automated analysis programs and searches through user home folders for the purposes of gathering statistical data and searching for security problems. These programs shall not investigate the contents of user data, nor search for particular files by name, but may report on configuration problems or hazardous account or permission settings.
3. All users of Bancroft School computer systems must be aware that system errors and other exceptional conditions may sometimes result in private data (including e-mail) being exposed to parties for which they were not intended. This is an unavoidable consequence of using shared computer systems.
4. Users are expected to make an effort in good faith to not examine data for which they were not meant to have access. Users are also expected to be aware of the risks and to not store truly sensitive personal information on the Bancroft School computers or network.
5. All users of Bancroft School computer systems must be aware that much operational data about users' activities is logged or otherwise recorded in places visible to system administrators and sometimes to all users of the system or even to the general public. This is an unavoidable consequence of using shared computer systems. Users are expected to be reasonably aware of the risks and to **not conduct** activities they would not want appearing in these records. Users with concerns or questions are encouraged to contact the Director of Technology.
6. All users are responsible for their own actions. Bancroft School endorses no action by virtue of the action-taking place on or involving a Bancroft School computer.