NEW BEGINNINGS
SCHOOLS FOUNDATION

Technology Acceptable Use Policy

Purpose

To ensure Information Technology (IT) infrastructure that promotes a reliable, safe and secure technology enriched teaching and learning environment.

Policy

Acceptable Use of IT Systems: This policy sets forth general parameters of acceptable use of IT systems. Individual school administrators may, at their discretion, implement and enforce stricter controls than those required by this policy.

1. **Acceptable Use.** IT systems may be use only for their authorized purposes – that is, to support the education, administrative and other functions of the Charter School "Network". For internet specific policy, please refer to Acceptable Use of Internet Policy.
2. **Proper Authorization.** Users are entitled to access only those elements of the IT Systems that are consistent with their authorization.
3. **Prohibited Use.** The following categories are unacceptable and prohibited:
    a. **Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others**. Users must not deny or interfere with or attempt to deny or interfere with service to other users in any way, including by "resource hogging," misusing mailing lists, propagating "chain letters" or virus hoaxes, "spamming". Knowing or reckless distribution of unwanted mail or other unwanted messages is prohibited. Other behavior that may cause excessive network traffic or computing load is also prohibited.
    b. **Harassing or threatening use**. This category includes, for example, discriminatory harassment, display of offensive, sexual material in the school or workplace and repeated unwelcome contacts with another.
    c. **Use damaging the integrity of Network or other IT Systems**. This category includes, but is not limited to, the following six activities:
        i. **Attempts to defeat system security**. Users must not defeat or attempt to defeat any IT System's security – for example, by "cracking" or guessing and applying the identification or password of another User, or compromising room locks or alarm systems. (This provision does not prohibit, however, Systems Administrators from using security scan programs within the scope of their Systems Authority.)
        ii. **Unauthorized access or use**. The network recognizes the importance of preserving the privacy of Users and data stored in IT systems. Users must honor

this principle by neither seeking to obtain unauthorized access to IT Systems, nor permitting or assisting any others in doing the same. Users are prohibited from accessing or attempting to access data on IT Systems that they are not authorized to access. Furthermore, Users must not make or attempt to make any deliberate, unauthorized changes to data on an IT System. Users must not intercept or attempt to intercept or access data communications not intended for that user, for example, by "promiscuous" network monitoring, running network sniffers, or otherwise tapping phone or network lines.

iii. **Disguised use**. Users must not conceal their identity when using IT Systems, except when the option of anonymous access is explicitly authorized. Users are also prohibited from masquerading as or impersonating others or otherwise using a false identity.

iv. **Distributing computer viruses**. Users must not knowingly distribute or launch computer viruses, worms, or other rogue programs.

v. **Modification or removal of data or equipment**. Without specific authorization, Users may not remove or modify any NBSF-owned or administered equipment or data from IT Systems.

vi. **Use of unauthorized devices.** Without specific authorization, Users must not connect networking equipment (routers, hubs, sniffers, etc.) to the Campus network, nor operate network services software (routing, sniffing, name service, multicast services, etc.) on a computer attached to the network, nor physically or electrically attach any additional device (such as an external disk, printer, or video system) to IT Systems.

d. **Use in violation of law**. Illegal use of IT Systems -- that is, use in violation of civil or criminal law at the federal, state, or local levels -- is prohibited. Examples of such uses are: promoting a pyramid scheme; distributing illegal obscenity; receiving, transmitting, or possessing child pornography; infringing copyrights; and making bomb threats. With respect to copyright infringement, Users should be aware that copyright law governs (among other activities) the copying, display, and use of software and other works in digital form (text, sound, images, and other multimedia). The law permits use of copyrighted material without authorization from the copyright holder for some educational purposes (protecting certain classroom practices and "fair use," for example), but an educational purpose does not automatically mean that the use is permitted without authorization.

e. **Use in violation of Network contracts**. All use of IT Systems must be consistent with Network and New Beginnings School Foundation (NSBF) contractual obligations, including limitations defined in software and other licensing agreements.

f. **Use in violation of Network policy**. Use in violation of other applicable Network policies also violates this acceptable use policy (AUP). Relevant policies include, but are not limited to, harassment of a sexual or any other nature, as well as, departmental, and work-unit policies and guidelines regarding incidental personal use of IT Systems.

g. **Use in violation of external data network policies**. Users must observe all applicable policies of external data networks when using such networks.

Enforcement Procedures

1. A. **Complaints of Alleged Violations**. An individual who believes that he or she has been harmed by an alleged violation of this Policy may file a complaint with their supervisor or teacher. The individual is also encouraged to report the alleged violation to the authority overseeing the facility most directly involved who must investigate the allegation and (if appropriate) refer the matter to Network authorities for disciplinary action
2. **Reporting Observed Violations**. If an individual has observed or otherwise is aware of a violation of this Policy, but has not been harmed by the alleged violation, he or she may report any evidence to the authority overseeing the facility most directly involved, who must investigate the allegation and (if appropriate) refer the matter to Network authorities for disciplinary action.
3. **Disciplinary Procedures**. Systems Administrators are authorized to personally investigate and/or designate others to investigate alleged violations of this policy. Results of investigations will be submitted to Charter Network authority with recommendations for follow-up activities
    a. Repeat minor violations of this policy will result in the loss of use of technology resources
    b. Any violation of this policy that is also a violation of the law will in all cases be reported to the proper public authorities
    c. For Charter Network employees:
        i. Disciplinary action for violations range from simple verbal reprimand to termination depending upon the severity or impact of the violation
        ii. Any violation of this policy that is also a violation of any law will be reported to the proper public authorities
    d. For students: Disciplinary action for violations will be determined by the appropriate school authorities
4. **Legal Liability for Unlawful Use**. In addition to NBSF discipline, Users may be subject to criminal prosecution, civil liability, or both for unlawful use of any IT System.
5. **Appeals**. Users found in violation of this Policy may appeal or request reconsideration of any imposed disciplinary action in accordance with the appeals provisions of the relevant disciplinary procedures.

Policy Amendments

This policy may be amended to reflect changes deemed necessary by NBSF. Amendments will be updated and shared throughout NBSF via googledocs.

This policy samples heavily from the University of New Orleans "Acceptable Use Policy for Information Technology", omitting or adapting certain sections as deemed necessary for the different educational and technological environment.

Gilbert Bennett
Chief Operations Officer