THOMAS JEFFERSON INDEPENDENT DAY SCHOOL
INFORMATION AND COMMUNICATION SYSTEMS USAGE POLICY

THOMAS JEFFERSON INDEPENDENT DAY SCHOOL (TJ) Information and Communication Systems (the "Systems") (*including, but not limited to, computers, computer accounts, dial-in systems, telephones, voice mail, e-mail, Internet, Intranet and electronically written messages, memos, notices or other forms of communication capable of being transmitted between two or more people or computers*) are provided for the use of authorized TJ students, employees, contractors, visitors and approved temporary services personnel (the "users") only. The Systems should be used for TJ business and educational purposes, and in accordance with all applicable laws, regulations and internal TJ business policies. Unauthorized, improper or illegal use of the Systems will result in disciplinary action, up to and including expulsion or termination of employment.

Permissible Uses

• TJ'S Systems are provided for use in TJ business-related and education-related activities. Incidental and occasional personal use should be minimized, and must comply with all applicable TJ policies. Restrictions on personal use by students shall be in TJ'S sole discretion and students should have **no expectation of privacy regarding their personal use** of the TJ systems. All System usage, business and personal, is subject to retrieval and review by TJ.

Prohibited Uses

TJ'S Systems shall not be used in the following manners:

• To view, access, upload, download, store, transmit, create or otherwise manipulate any fraudulent, harassing, offensive, pornographic or other sexually explicit or obscene materials, images or messages.
• To solicit or distribute messages or information for political causes.
• For any commercial purposes unrelated to the business of TJ.
• For gambling or playing interactive networked games.
• For excessive use of streaming data, audio or video, such as ticker tape updates. Web sites of this type should be accessed only when required for educational purposes.
• To send messages, data, documents or programs which are prohibited by any federal, state or local law or regulation.
• To intentionally "capture and open" electronic communications intended for others, except as required for authorized personnel to diagnose and correct delivery problems.
• To "spoof" or construct a communication so it appears to be from another person.
• To "snoop" or obtain access to files or communications of others.
• To use loopholes or tools to circumvent the Systems or network security, the knowledge of special passwords, or the covert acquisition of passwords in order to damage the Systems, obtain extra resources; take resources from another user, or gain access or control of any system for which proper authorization has not been granted.
• To copy, alter, transmit or store any materials protected by copyright, patent, trade secret or other form of legal protection without proper authorization. The use of software on a local area network or on multiple computers must be in accordance with a license agreement.
• To upload, distribute or copy any software licensed to TJ, or data owned or licensed by TJ, without the express authorization from the manager responsible for the software or data.
• To install TJ owned or licensed software on home or other computers not owned or leased by TJ, without the prior approval of TJ'S director of technology.
• To use any Systems, including but not limited to cellular phones, while operating a vehicle. If there are times when it is absolutely necessary to use a phone while driving, obtain and use hands-free equipment to permit both hands to remain on the wheel and keep attention on the road while using the phone.

Monitoring/Filtering and Privacy

• TJ reserves the right to access, monitor and record any use of the Systems and any information electronically created, stored or transmitted on the Systems, without the knowledge or consent of the user. TJ will comply with all applicable laws and may report any illegal usage of the Systems to the appropriate federal, state and/or local authorities. **No user should have any expectation of privacy regarding the use of the Systems** and no communication on the Systems is considered private. The existence of passwords or other means to prevent access shall not restrict or restrain TJ's right to access the Systems.

• Access to and usage of the Systems may be monitored and/or audited without notice. TJ has software and systems in place that monitor and log all Internet usage. Security systems are capable of logging (for each and every user) each website visit, each chat, newsgroup or email message, and each file transfer into and out of TJ internal networks. Internet activity is subject to review and analysis for usage patterns and for violations of this Policy.
• Special software is also installed on TJ'S Systems in order to support resource usage, accounting, security, network management, hardware and software inventory and software updating functions and to provide better support to students and faculty.
• Commercial filter packages may be installed on the network to restrict access to certain types of sites. It is a violation of this Policy to circumvent or attempt to circumvent any such filters. If a user is blocked from a site they believe is necessary for business purposes, the user may contact TJ'S director of technology and request that the blocking of the site be removed. If a user should inadvertently connect to a site containing prohibited material, the user should disconnect from the site immediately, regardless of whether access to the site had been permitted by any screening or rating program.

Internet Connections
• Users may not establish Internet or any network connections that could allow unauthorized persons to gain access to TJ'S Systems. These connections include, but are not limited to, establishment of hosts, public modem dial-ins, wireless access points, World Wide Web home pages and File Transfer Protocol ("FTP"). Any and all access to TJ'S Systems must be approved by TJ'S director of technology.

User Conduct
• Any user who is aware of or suspects any violation of this Policy shall immediately report such violations to their direct supervisor and/or the director of technology.
• Each user using TJ'S Systems shall use only their authorized passwords and access information issued to them by TJ. Unauthorized use of other passwords or access information will result in immediate discipline, up to and including expulsion or termination.
• IT IS A VIOLATION OF THIS POLICY TO ATTEMPT TO DISABLE, DEFEAT OR CIRCUMVENT ANY TJ SECURITY SYSTEM.
• USERS SHALL NOT DISPLAY, SHARE OR STORE PASSWORDS ONLINE, IN AN UNSECURE LOCATION, IN BATCH FILES, MACROS, APPLICATIONS, ICONS OR BY OTHER METHODS EASILY ACCESSIBLE TO OTHERS.

Ownership
• TJ'S Systems and all information electronically created, stored (including personal files, whether password protected or not) or transmitted on the Systems are the property of TJ and TJ owns all rights thereto.

I have read and hereby agree to comply with the Thomas Jefferson Independent Day School Information and Communication Systems Usage Policy.

Student Name: _____

Student Signature: _____ Date: _____

As parent/legal guardian of the student named above, I grant permission for my child to access networked computer services such as electronic mail and the Internet. I understand that this access is designed for educational purposes. I understand The School uses an industry standard provider for Internet content filtering services, and I understand that data accessed from the Internet is not necessarily provided by The School. I will not hold the school responsible for materials acquired on the network. I have read and agree to the Thomas Jefferson Independent Day School Information and Communication Systems Usage Policy, and I understand that I may be held responsible for violations by my child.

Parent/Guardian Name: _____ Daytime Phone: _____

Parent/Guardian Signature: _____ Date: _____