ACCEPTABLE USE REGULATIONS FOR EMPLOYEES

1. INTRODUCTION.

The Solvay Union Free School District technology services exist to support the educational mission of the District. The District will provide District employees and Board members with access to various technology resources. This will include software, hardware, communication networks including E-Mail, and Internet access. It may also include the opportunity for some District personnel to have independent access to District technology services from remote locations. All of these uses are subject to this regulation.

The Superintendent or his/her designee will provide District personnel with training in the proper and effective use of the District's technology services.

Employee use of District technology services is conditioned upon this agreement (written or electronic) by the employee and the District. The requirements of this regulation are designed to insure acceptable use by all parties. This agreement shall be kept on file and renewed annually.

Generally, the same standards of acceptable District employee conduct which apply to any aspect of job performance shall apply to use of the District technology services. Employees are expected to communicate in a professional manner consistent with applicable polices and regulations. District technology services are not to be utilized to disclose confidential information about students or other employees to unauthorized persons.

District employees shall adhere to the laws, policies, and rules governing technology resources including, but not limited to, copyright laws, rights of software publishers, license agreements, and rights of privacy created by federal and state laws.

District employees who engage in unacceptable use may lose access to the District technology services and may be subject to further discipline under the law or policy in accordance with applicable collective bargaining agreements. Legal action may be initiated against District employees who willfully, maliciously, or unlawfully damaged or destroy District property or data.

Each Employee who uses the District's technology services agrees to Board of Education Policy 6410: STAFF USE OF COMPUTERIZED INFORMATION RESOURCES (i.e. ACCEPTABLE USE POLICY) and the accompanying regulations (i.e. ACCEPTABLE USE REGULATIONS FOR EMPLOYEES).

2. **PRIVACY RIGHTS**
   All E-mail files, electronic data, and storage media posted, created, maintained or stored on district technology shall remain District property subject to District control and inspection at its discretion. The Superintendent or his/her designee may access all such files and communications to ensure system integrity and to ensure employees are complying with requirements of BOARD OF EDUCATION POLICY 6410 and these regulations. **All use of District technology services is audited for acceptable use.** District personnel should **NOT** expect that information shared over or stored in any manner on District electronic media will be private. All District policies governing behavior and communications apply to employee use of District technology services.

3. **MINIMAL PERSONAL USE.**
   Acceptable use of District technology services are those that conform to the purposes, goals, and mission of the District and to each users job duties and responsibilities. The District understands that on occasion an employee may need to use District technology services (specifically E-Mail and/or Internet access) for personal reasons (e.g. family correspondence). This minimal personal use is acceptable as long as it does not diminish the employee's productivity, work product, or ability to perform services for the District. Examples of acceptable personal use include but are not exclusive to:
   a. ORDERING MERCHANDISE.
      Using the District technology services to order personal online merchandise through an online reseller.
   b. PERSONAL RESEARCH
      Using the District technology services to engage in personal research such as but not exclusive to news or blogs.
   c. ACCESSING E-MAIL FROM ANOTHER EDUCATIONAL INSTITUTION.
      Employees enrolled at an institution of higher education may access their student E-Mail account to engage in educational correspondence.
   d. OTHER USES.
      However, staff may not use the District technology services to engage in any activity mentioned in SECTION 5 of this regulation.

NOTE: <u>All</u> use, including personal use, of the District technology services is audited for acceptable use.

4. **STORING OF PERSONAL INFORMATION**
   Users should not save personal information such as personal credit card numbers or other forms of personal identification on District technology services.
   Information posted or stored on District technology services is not considered private.

5. **VIOLATIONS OF DISTRICT ACCEPTABLE USE**

The District employs auditing technologies to monitor all activity on the District technology services. The District will cooperate with legal authorities and/or third parties in the investigation of any suspected or alleged crime or civil wrong. Violations of this regulation may result in the suspension or termination of access to the District technology services, and/or disciplinary action in accord with applicable law and District policy. The following constitute violations of this acceptable agreement:

a. ONLINE GAMING IS PROHIBITED (INCLUDING GAMBLING)
An exception is when an online game is part of a classroom activity assigned by a teacher and has an educational purpose.

b. THEFT OR VANDALISM.
This includes but is not limited to the stealing or theft of software, and/or hardware. It also includes unauthorized modification and/or the destruction of computer software or hardware as well as the intentional misuse of district equipment.

c. ILLEGAL USE.
Using the District technology services to transmit any material (by E-Mail, uploading, posting, or otherwise) that intentionally or unintentionally, violates district policies and/or any applicable local, state, or federal law is prohibited.

d. CAUSING HARM TO MINORS.
Using the District technology services to harm, or attempt to harm, minors in any way is prohibited.

e. ACCESSING OR DISTRIBUTING THREATENING AND/OR OBSCENE MATERIALS.
    i. Using the District technology services to transmit any material (by E-Mail, uploading, posting, or otherwise) that threatens or encourages bodily harm, destruction of property, or disrupts the functions of District business is prohibited.
    ii. Materials determined to be obscene including accessing or distributing pornography via the District's technology services is prohibited. This includes "sexting" or the sending of pornographic images or text. Transmitting of pornographic or obscene images of minors is both a state and federal crime.
    NOTE: If a user accidentally accesses an inappropriate site, as soon as practicable he/she should bring that site to the District's attention.

f. HARRASSMENT.
Using the District technology services to transmit any material (by E-Mail, uploading, posting, or otherwise) that harasses others is prohibited.

g. FRAUDULANT ACTIVITY.
Using the District technology services to make fraudulent offers to sell or buy products or other services is prohibited.

h. FORGERY AND/OR IMPERSONATION
    i. Adding, removing or modifying identifying network header or identifying information in an effort to deceive or mislead is prohibited.

ii. Using someone else's account or allowing someone else to use your account is prohibited.
iii. Attempting to impersonate any person by using forged headers or other identifying information is prohibited.

i. HACKING
Hacking is a Federal offense. It includes the use of District technology services to access, or to attempt to access, or the attempt to penetrate, security measures of the District or another entity's computer software or hardware, electronic communications system, or telecommunications system. This is regardless of whether or not the intrusion results in the corruption or loss of data. This includes deliberately going into off limit service areas (e.g., hard drive or "C:" drive, "Default Profile," "Network Neighborhood," and those services requiring administrative rights).

j. PLAGIARIZING COPYRIGHTED MATERIALS OR TRADEMARK INFRINGMENT
Using the District technology services to download, transmit, or copy any material (by E-Mail, uploading, posting, or otherwise) that infringes any copyright, trademark, patent, or other proprietary rights of any third party is prohibited. This includes, but is not limited to, the unauthorized copying of copyrighted material; the digitization and distribution of photographs from magazines books, or other copyrighted sources; the coping or unauthorized transmittal of copyrighted software, music, or other digital media.

k. COLLECTION OF PERSONAL DATA
Using the District technology services to collect, or attempt to collect, personal information about third parties without their knowledge or consent is prohibited.

l. RESELLING AND/OR USING THE DISTRICT TECHNOLOGY SERVICE FOR COMMERICAL PURPOSES.
Reselling the District technology services or using the District technology services for commercial activities is prohibited. Using a district user account for commercial use is prohibited. The District technology services are intended to support the educational process and/or official school business.

m. CAUSING NETWORK DISRUPTIONS AND/OR ENGAGING IN UNFRIENDLY ACTIVITY.
Using the District technology services for any activity which adversely affects the ability of other people or systems to use of the service is prohibited. This includes "denial of service" (DoS) attacks against another network host or individual employees, or deliberately infecting the District technology services with a virus, worm, Trojan horse, or other malicious software. Interference with or disruption of other network employees, network services or network equipment is prohibited. Downloading or loading software applications on the hard drive ("C:" drive) or network drive ("H:" drive) is considered an unfriendly activity.

n. LONG CONNECTIONS
Using a District account for high volume or commercial use is prohibited. Users may stay connected so long as they are actively using that connection for educational or business purposes. Accordingly, the District maintains the right to terminate any connection following an extended period of inactivity as determined by the District.

o. ABUSE OF PRINTING SERVICES
District printers should only be used to print minimal copies of materials either required to support the educational process and/or for official school business. Multiple copies of print materials should be done using either building photocopiers or sending the materials to the BOCES Copy center. **All district printing is monitored.** Abuse of district printing services may involve additional disciplinary action.

6. E-MAIL AND ONLINE COMMUNICATION STANDARDS.

E-Mail is a valuable business communications tool when used in a responsible, effective, and legal manner. Although E-Mail is perceived as less formal that other written communications, the same laws and business record requirements apply. The District established the E-Mail system for business communication, including those in which students or student issues are discussed. Every user has the responsibility to maintain the District's reputation and shall be familiar with acceptable use of E-Mail to avoid placing either themselves or the organization at risk:

a. ACCEPTABLE USE
All guidelines described in SECTION 5 of this regulation apply to the acceptable use of District E-Mail.

b. PRIVACY AND MINIMAL PERSONAL USE.
No E-Mail or other form of electronic communication should be considered private. The District E-Mail system may be used for occasional personal use as stated in SECTION 3. However, this personal use shall not include the distribution of chain letters, junk mail, or jokes. **All District E-Mail may be audited for acceptable use and is archived according to federal court guidelines.**

c. SENDING UNSOLICITED E-MAIL/UNSOLICITED BULK E-MAIL.
Using the District technology services to transmit of facilitate the transmission of any unsolicited E-Mail or unsolicited bulk E-Mail is prohibited.

d. ELECTRONIC MESSAGES.
Any message posted on a Web Log (blog), Newsgroup Forum, or Web site or other electronic site or forum should be considered public and permanent. All such postings shall be limited to school-based educational use only.

e. SYSTEM AUDITING AND ARCHIVING
As stated earlier, **there is no expectation of privacy in the use of the District's E-Mail system**. The District maintains an E-Mail archiving server, which will keep a copy of all sent and received E-Mail. Backup and recovery of all E-Mail data will be included in the District's backup and

disaster recovery management strategy. No E-Mail will be purged if it is under consideration of a court or has a litigation hold on the data. Access to your primary archive is available. Access to the primary E-Mail account of another active user will be available with the appropriate administrative authorization. The ability to search the E-Mail archive of other users will only be done with the authorization of the Superintendent or his/her designee.

f. E-MAIL ETIQUETTE SHOULD BE FOLLOWED
   i. Include a meaningful, clear subject line.
   ii. As with all written correspondence, District E-Mails should begin with a proper salutation and close with a "Thank-you" (or other appropriate closure) and the user's electronic signature.
   iii. Use proper grammar and etiquette.
   iv. Use standard spelling, punctuation, and capitalization. (Plz dnt abbrvt or uze txt msg lngo)
   v. Messages should not be written in ALL CAPS. (THERE IS NOTHING WORSE THAN E-MAIL SHOUTING.)
   vi. Be brief, direct, polite, and to the point.
   vii. Responses requiring a long E-Mail merit a face-to-face conversation.
   viii. Use cc: (carbon copy) and bcc: (blind carbon copy) sparingly and as appropriate.

7. USE OF PERSONAL ELECTRONIC DEVICES/TELEPHONE USE.

a. DEFINITION.
   Personal Electronic Devices include any device not owned by the district and may include but are not exclusive to:
   i. Personal computers, laptop computers, netbooks, or portable gaming systems;
   ii. cell phones;
   iii. digital cameras or video recorders;
   iv. personal digital assistants (PDAs);
   v. Digital Players (MP3 devices, iPods, etc);
   vi. And all other digital media devices.

b. ACCEPTABLE USE OF PERSONAL ELECTRONIC DEVICES:
   Connecting any Personal Electronic Device to District technology services is prohibited. All topics listed in SECTION 5 of this regulation apply to the acceptable use of Personal Electronic Devices.

c. INDEMNITY
   The District is not responsible for the theft, loss, or damage that may occur while these Personal Electronic Devices are on school grounds, District transportations systems, and/or while attending District sponsored activities or functions.

8. PERSONAL PORTABLE STORAGE DEVICES:

a. DEFINITION
Personal storage devices include but are not exclusive to:
   i. USB Storage Devices ("Thumb/Flash Drives");
   ii. CD/DVD-ROMS,
   iii. Flash memory cards;
   iv. 3.5 "Floppy" Disk or other removable media.

b. ACCEPTABLE USE
Users may connect personal storage devices to District technology services provided the devices do not attempt to install software on a District computer and map correctly to the District system.

c. STORAGE OF CONFIDENTAL INFORMATION
Confidential data may not be copied to a personal storage device without the prior written authorization of the Superintendent. Use of Personal Storage Devices to copy or transport confidential information such as but not exclusive to: student or employee biographical or health data, student Individualized Education Plans (IEPs), etc. is prohibited.

9. USE OF DISTRICT LAPTOPS OR PORTABLE COMPUTING DEVICES.

The District may assign a laptop or Portable Computing Device (District laptop) to an employee to support specific District activities, programs, or functions. The assigned District laptop computer is the property the District and will be managed by District support personnel. **All District assets, such as a District laptop, are audited for acceptable use.** Employees assigned a District laptop are expected to follow the guidelines listed below:

a. ACCEPTABLE USE
All guidelines described in SECTION 5 of this regulation apply to the acceptable use a District laptop.

b. USE OF DISTRICT LAPTOP FOR MIMINAL PERSONAL USE
The district understands that an employee assigned a District laptop may need to use the device to engage in personal reasons (e.g. family correspondence). The District laptop may be used for *minimal personal use* as outlined in SECTION 3 of this regulation. This includes but is not exclusive to:
   i. Using the laptop to order personal online merchandise through an online reseller.
   ii. Using the laptop to engage in personal research such as but not exclusive to news or blogs.
   iii. Using the laptop to access personal E-Mail accounts, Skype, or other forms of electronic messaging. **All forms of electronic communication on the District laptop are audited for acceptable use.**

c. SECURITY.
The employee assigned a District laptop is responsible for the safety and security of the District laptop at all times. The District laptop is to be kept in a locked cabinet or locker onsite when not in use. The District laptop may be taken home overnight when needed.

d. REPORT THEFT, DAMAGE, OR LOSS IMMEDATELY.
    i. Theft (or the suspected theft) of a District laptop must be reported immediately to the District along with the filling of an official police report.
    ii. Any damage to a District laptop, or malfunctioning of a District laptop, must be reported to District support personnel immediately.
    iii. The user accepts responsibility for any costs that can be attributed to negligence, intentional misuse, or the loss of a laptop/computer and/or all peripheral items. This includes leaving a District laptop in a car in which either theft or damage due to temperature could occur.
e. TAMPERING WITH DISTRICT ASSETS.
    i. The removal of, or alteration to, any District identification labels attached to, displayed on, or stored in a District laptop is prohibited.
    ii. Modification of user accounts found on a District laptop is prohibited. No addition or deletion of any user account is allowed on a District laptop except by designated District support personnel.
    iii. Software or hardware (except for mice, keyboards, speakers/headphones, or portable storage devices) shall not be installed or removed from a District laptop. Except for pre-configured automatic system updates, only District support personnel may remove or install software or hardware on a District laptop.
    iv. Modification of either District laptop anti-virus software and/or the firewall system is prohibited.
    v. All District laptops will need periodic upgrades and/or repairs. Only District support personnel shall perform these tasks.
f. TURN IN THE LAPTOP WHEN REQUESTED.
    Upon request, a District laptop must be returned promptly regardless of reason.
    i. Private or personal information should not be stored on a District laptop.
    ii. A District laptop may need to be restored to its original settings, and that all work files may be lost during the restore process.
    iii. All contents of a District laptop may be accessed at any time as deemed necessary by either District support personnel or Administrations.
g. AUTHORIZED EMPLOYEES
    District laptops are to be used only by authorized District employees.
h. STORAGE OF CONFIDENTAL INFORMATION
    Confidential or biographical student data may not be stored on a District Laptop without the prior written authorization of the Sup. Use of a District laptop to copy or transport confidential information such as student biographical or health data, or student Individualized Educational Plans (IEPs), etc. is prohibited.

i. OFFSITE WIRELESS ACCESS
District laptops maybe connected to an offsite, wireless network, provided that the site does not require the installation of software, modify the preset firewall configuration, or change any of the District network settings on the laptop. (NOTE: Connecting to an unsecure wired or wireless access point may compromise of all information on the laptop.)

j. FREQUENTLY BACKUP
It is the employee's responsibility to make regular backups of District laptop files to an external device such as a USB drive, CD/DVD, or to the District file server. All files housed on the District laptop and/or on the school server are the property of the District and may be accessed at any time by District support personnel or the administrators. Failure to make regular backups can result in the loss of data.

k. DISTRICT PROPERTY
All District Laptops are the property of the District. If an employee leaves the District, the District laptop will be returned immediately to the District in working order.

10. REVISIONS TO THIS ACCEPTABLE USE AGREEMENT.
The District reserves the right to revise, amend, or modify this Agreement, and other policies and agreements at any time and in any manner. Notice of any revision, amendment, or modification will be posted in accordance with District policy.

[Note: Sign off to be on a separate sheet and signed at the start of each school year.]

Acknowledgement of Responsibilities (employee reads and signs**):**

I have received and reviewed the Solvay Union Free School District ACCEPTABLE USE REGULATIONS FOR EMPLOYEES and agree to abide by the terms and conditions for acceptable use of the District Technology Services including access to the Internet. I further understand that a violation of the regulations is unethical and may constitute grounds for disciplinary action and/or appropriate legal action.

Name (**please print**): _____ Building:_____

Signature: _____ Date: __/__/__