TELECOMMUNICATIONS ACCESS AND ACCEPTABLE USE

Purpose

The purpose of this policy is to establish acceptable and unacceptable use of the Covered Electronic Resources provided by Indian River School District ("IRSD") and the State of Delaware (collectively with IRSD, the "District"), to Covered Users. Electronic Resources are provided for a limited education purpose for students and to facilitate employees' work productivity. This policy serves to ensure that actual use conforms to this intended purpose.

Related Policies

This Policy is intended to supplement other applicable policies and standards. Specifically, the State of Delaware's Acceptable Use Policy (DTI-0042.02), Information Security Policy (SE-ESP-001), and Strong Password Authentication Standard (SE-PWD-001), each as amended, and IRSD policies regarding Student conduct, Staff conduct, and other applicable policies that apply to the use of Electronic Resources and are not replaced by this Policy.

SCOPE

Covered Technology

This policy applies to "Electronic Resources," which are those resources that are: (a) provided by the District; (b) paid for, in whole or in part, by the District; (c) used to conduct business or other activity for or on behalf of the District; or (d) used inside or outside a District facility. Covered Electronic Resources include, without limitation, the following:

- "E-mail," which includes all electronic-mail accounts and services provided to Covered Users by the State of Delaware or IRSD;
- "Electronic Resources," which includes all computers and related resources whether stationary, portable or Internet-based (i.e., stored in the "Cloud"), including but not limited to all related peripherals, components, disk space, storage devices, servers, and output devices such as telephones, hand-held devices, printers, scanners, and copiers, whether owned or leased by the District;
- "IRSD Network," which includes the infrastructure used to transmit, store, and review data over an electronic medium, and includes any and all of the following technologies provided to authorized users: (a) Internet service; (b) intranet system; (c) IRSD mainframe system; and (d) any collaboration systems, including but not limited to calendaring, message boards, conference boards, blogs, text messaging, instant messaging, video conferencing, websites, and podcasting, whether the system is owned or contracted;
- "Electronic Data," which includes any and all information, data, and material, accessed or posted through any Electronic Resource; and
- Personal Communication Devices," which includes any cellular phone, smart-phone, or other personal electronic communication device.

Covered Users

This policy applies to all "Covered Users," which is defined to include all of the following:

- Employees, contractors, consultants, temporary, and other workers at the District, including all personnel affiliated with third parties;
- IRSD board members and officers;
- Volunteers and interns performing work for or otherwise acting on behalf of the District; and
- IRSD students.

General Guidelines for Use

The following guidelines summarize the principles underlying this Policy and serve as an effective baseline for evaluating whether a particular use violates those principles.

- Electronic Resources are not intended for public access. The District has the right to place reasonable restrictions on the use of Electronic Resources.
- Users are required to observe all rules and obligations set forth elsewhere by the District (for example, in the Board of Education Policy Manual or Student-Parent Handbook) or by law at all times. This policy is intended to supplement, not replace, those duties.
- Access to and use of Electronic Resources is a privilege, not a right. Parent or guardian permission is required for all students under age 18.
- As set forth in more detail in Section 9, below, the District reserves the right to monitor any and all use of Electronic Resources with or without additional notice to or consent by an affected User.
- Users will be responsible for any and all damage caused by their use of Electronic Resources where such use does not comply with the requirements or purposes of this Policy. Responsibility may take the form of financial compensation, discipline, and/or restrictions on further use, as appropriate under the circumstances.

DUTIES

All Users

It shall be the responsibility of supervising staff to educate, supervise, and monitor appropriate usage of the IRSD Network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, the Children's Online Privacy Protection Act and the Protecting the children in the 21st Century Act. All Users have a duty to protect the security, integrity, and confidentiality of Electronic Resources, including the obligation to protect and report any unauthorized access or use, abuse, misuse, degradation, theft, or destruction. Users shall comply with this Policy and all other applicable policies, rules, and laws, when using Electronic Resources.

District officials are responsible for designating Users authorized to use Electronic Resources. District officials will approve access to Electronic Resources by Users who are not District employees or students, such as consultants or contractors, only when access is required for the User to perform critical functions and services and only upon the User's execution of a confidentiality agreement regarding such access and use. Procedures for disabling or otherwise modifying any technology protection measures shall be the responsibility of Technology Manager or designated representatives.

The Director of Instruction or designated representatives will provide age-appropriate training for Students who use Electronic Resources ("Training"). Training provided will be designed to

promote the District's commitment to: (a) The standards and acceptable use of Electronic Resources as set forth in this Policy; (b) Student safety with regard to: (i) safety on the Internet; (ii) appropriate behavior while on online, social-networking sites, and in chat rooms; and (iii) cyber-bullying awareness and response; and (c) compliance with the E-rate requirements of the Children's Internet Protection Act.

Students will receive Training, which shall provide education about Internet safety through the District's Internet-safety curriculum, as required by the Protecting Children in the 21st Century Act and regulated regulations. This Training includes education about appropriate online behavior, including: (a) safety on the Internet; (b) interacting with other individuals on social networking websites and in chat rooms; and (b) cyber-bullying awareness and response. Students will acknowledge receipt of the Training, that the Student understood the Training, and that the Student agrees to follow the provisions of the District's policies regarding acceptable use of Electronic Resources.

Students have a duty to take reasonable steps to protect their privacy and personal information when using Electronic Resources. Students must not disclose personal contact information, except to educational institutions for educational purposes, without prior advance approval. Students also must promptly disclose to a teacher or other appropriate District employee any violation of this Policy, including any message received that the student believes to be inappropriate or makes the student feel uncomfortable.

Personnel

District employees are required to only communicate with students through District-provided forms of communications (such as email, learning management systems, or other online collaboration platforms) and are forbidden from using other forms of personal electronic communication with students, such as Instant Messaging, cellular phones, social media or texting. District employees are required to take reasonable measures to protect their personal information and reputation when using Electronic Resources or otherwise participating in activity online.

Ownership

All Electronic Data, such as documents, data, and information that is stored, transmitted, and processed on the IRSD Network or Electronic Resources are the property of the District. When a User is no longer affiliated with the District as an employee or contractor all information stored by that User on any Electronic Resource remains the property of the District.

UNACCEPTABLE USES

Preventative Measures

To the extent practical, technology protection measures (or "Internet filters"), shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material

deemed harmful to minors (i.e., children under the age of majority). Subject to staff supervision, technology-protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

To the extent practical, steps shall be taken to promote the safety and security of Covered Users when using the IRSD Network. Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Access to Inappropriate Material

It shall be a violation of this Policy for any User to use any Electronic Resource to upload, post, mail, display, store, access, or transmit, any Inappropriate Material. Inappropriate Material is defined as any content, communication, or information that conflicts with the fundamental policies and mission of the District. Whether material or content is considered Inappropriate shall be determined without regard to whether such material or content has been blocked by any filtering software used by the District.

Examples of Inappropriate Material include, but are not limited to, material that:

- is hateful, harassing, threatening, libelous, or defamatory or considered bullying in nature;
- is deemed offensive or discriminatory based on race, religion, gender, age, national origin, citizenship, sexual orientation, gender identity, color, creed, mental or physical disability, marital status, or other characteristic protected by state, federal, or local law;
- constitutes use for, or in support of, any obscene or pornographic purpose including the transmission, review, retrieval, or access to any profane, obscene, or sexually explicit material;
- constitutes use for the solicitation or distribution of information intended or likely to incite violence, cause personal harm or bodily injury, or to harass, threaten, or stalk another individual
- solicits or distributes information with the intent to cause personal harm or bodily injury;
- promotes or participates in a relationship with a student that is not related to academics or school-sponsored extracurricular activities, unless authorized in advanced by the student's parent or guardian and the appropriate IRSD official(s);
- promotes or participates in any way in religious or political activities;

Unlawful Purposes

It shall be a violation of this Policy for any User to use any Electronic Resource for any purpose that:

- constitutes or furthers any unlawful activity;
- gives rise to civil liability under any applicable law, including U.S. patent, trademark, or copyright laws, including copyrighted photos, clip art, or other images, including District or IRSD logos;
- impersonates any person, living or dead, organization, business, or other entity;
- enables or constitutes gaming, wagering, or gambling (includes fantasy football) of any kind;

- promotes or participates in any way in unauthorized raffles or fundraisers;
- engages in private business, commercial, or other activities for personal financial gain.

Security Violations

It shall be a violation of this Policy for any User to use any Electronic Resource in any way that threatens or violates the security of any Covered Technology, where such use:

- contains a virus, Trojan horse, logic bomb, malicious code, or other harmful component;
- constitutes a chain letter, junk mail, spam, or other similar electronic mail;
- constitutes unauthorized access or attempts to circumvent any security measures including the use of proxy anonymizers or any such tool that would allow for unfiltered access;
- obtains access to or use of another User's account, password, files, or data, or attempts to so access or use, without the express authorization of that other User;
- deprives a User of access to authorized access of Electronic Resources;
- engages in unauthorized or unlawful entry into a IRSD Network;
- shares e-mail addresses or distribution lists for uses that violate this Policy or any other District Policy;
- transmits sensitive or confidential information without appropriate security safeguards;
- falsifies, tampers with, or makes unauthorized changes or deletions to data located on the IRSD Network;
- obtains resources or IRSD Network access (production, guest, etc.) beyond those authorized both wired and wirelessly;
- distributes unauthorized information regarding another User's password or security data;
- discloses confidential or proprietary information, including student record information, without authorization;
- involves the relocation of hardware (except for portable devices), installation of peripherals, or modification of settings to equipment without the express prior authorization by the District Technology Department.
- installs, downloads, or uses unauthorized or unlicensed software or third-party system without the express prior authorization by the District Technology Department;
- involves a deliberate attempt to disrupt the IRSD Network.

Notice of Intent to Monitor

Users have no expectation of privacy in their use of and access to any Electronic Resource. District administrators and authorized personnel monitor the use of Electronic Resources to help ensure that uses are secure and in conformity with this Policy. The District reserves the right to examine, use, and disclose any data found on the IRSD Network in order to further the health, safety, discipline, or security of any student or other person, or to protect District property. It also may use this information in disciplinary actions and will furnish evidence of suspected criminal activity to law enforcement. In recognition of the need to establish a safe and appropriate computing environment, the District will use filtering technology to prohibit access, to the degree possible, to objectionable or unsuitable content that might otherwise be accessible via the Internet.

Limitation of Liability
The District makes no warranties of any kind, neither express nor implied, for the Internet access it provides. The District will not be responsible for any damages any User suffers, including but not limited to, loss of data. The District will not be responsible for the accuracy, nature, or quality of information stored on the IRSD Network, nor for the accuracy, nature, or quality of information gathered through District-provided Internet access. The District will not be responsible for financial obligations arising through the unauthorized use of the network.

Policy Violations
The District will cooperate fully with local, state, and federal officials, in any investigation related to any alleged or suspected illegal activity conducted through the IRSD Network.

Due Process
Any action taken in violation of this Policy will be subject to appropriate discipline, tailored to meet the facts and circumstances of the incident. Violations of this Policy may result in the revocation or suspension of access to the IRSD Network, as well as other disciplinary or legal action. Where a violation of this Policy also involves a violation of another District policy or rules, those policies or rules may affect the disciplinary action taken.

Student Violations
Violation of this Policy by a student may result in the revocation or suspension of access to the IRSD Network, as well as other disciplinary or legal action. All violations will follow the IRSD Student Code of Conduct. Other possible actions may include any combination of the alternatives as determined by the District which could include restitution, detention, probation, in-school alternative, suspension, referral to law enforcement, and expulsion depending on the severity of the violation and its applicability.

Employee Violations
Any employee who learns of or reasonably suspects a violation of this Policy is obligated to promptly report such information to his or her supervisor. Failure to do so is considered a separate violation of this Policy and, as such, may warrant disciplinary action.
All violations will follow the IRSD Staff Regulations Manual. Violation of this Policy by a District employee may result in the revocation or suspension of access to the IRSD Network. Violation may also result in other disciplinary or legal action, including but not limited to: reprimand, restitution, mandatory training or in-service, and termination depending on the severity of the violation and its applicability.

Instructional\Operational System Use
Due to the current or future use of online resources in regards to the instructional and operational needs of the district (email, learning management systems, online collaboration platforms, etc.) and the need to educate students about safe online practices a signature serves as validation of consent and gives permission for use of any aforementioned system.

Documentation
Upon review of the Policy a signature is required in which will be maintained via the personnel office for staff, volunteers, etc. Student's signature validation in regards to the policy will be maintained via the student information system.

Questions
Any questions about this Policy should be directed to the Director of Personnel and/or the Technology Manager.

Acceptable, Instructional and Operational Use Consent Form
I have read, understand, and will follow all rules, regulations, and policies when accessing and using the District's electronic information resources system. I further understand that any violation of the policy is unethical and may constitute a criminal offense. Should I commit any violation of the policy, I understand and agree that my access privileges may be revoked, and disciplinary action and/or legal action may be taken. I also understand that by signing I am agreeing to allow the use of any of the aforementioned systems for instructional or operational purposes by the district.

Employee	Name _____	Signature _____	Date _____
Student	Name _____	Signature _____	Date _____
Parent	Name _____	Signature _____	Date _____

Adopted 1/23/89
Revised 6/21/11, 6/19/12, 12/22/15, 2/27/17