Policy

Written Information Security Program

I. Objective

In order to protect personal information of residents of the State of Rhode Island (R.I.G.L. § 11-49.3-1), and if applicable, residents of the Commonwealth of Massachusetts (201 CMR § 17.00), and in compliance with any other applicable law or regulation (the "Regulations"), Chariho Regional School District ("Chariho") has developed the following Written Information Security Program (the "Program") to address the requirements of the Regulations.

The Program's goal is to set forth effective administrative, technical and physical safeguards applicable to personal information, to provide an outline for the ongoing compliance with the Regulations, to protect personal information from unauthorized access, use, modification, destruction or disclosure, and to position Chariho to comply with future privacy and security regulations as they may develop.

Personal information for purposes of this Program shall mean: the first name and last name or first initial and last name of an individual in combination with any one or more of the following data elements that relate to such individual:

(a) Social Security number;

(b) driver's license number, state-issued identification card number, passport number, tax payer identification number, alien registration number, or tribal identification number; or

(c) financial account number, credit card number, or debit card number with or without any required security code, access code, personal identification number or password, that would permit access to an individual's financial account, or deposit or savings account number, or medical information or health insurance information;

(d) medical information or health insurance information;

(e) unique biometric information (e.g. fingerprint, retinal scan); and/or

(f) a username or email address in combination with security code, access code or password or security question and answer that would permit access to an online account; provided however, that "personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

The safeguards set forth in this Program are meant to protect the security and confidentiality of personal information, and to protect against any anticipated threats or hazards to the security or integrity of personal information.

II. Information Security

In order to comply with applicable Regulations, we have appointed the Director of Information Technology and Information Systems and Human Resource Administrator who will be responsible for the following:

- Implementing the initial Program.
- Training employees who have exposure to personal information through their work at Chariho on the various aspects of the Program at least annually.
- Obtaining certification of attendance to and understanding of such training by the employees.
- Conducting regular testing and evaluation of the Program's safeguards.
- Verifying the ability of third-party recipients of personal information to comply with the Regulations.
- Reviewing the Program, its scope and its effectiveness at least annually or at such time as a material change in business practice occurs that implicates the security of personal information and upgrading information safeguards as necessary to limit risk.

III. Risk Assessment

The Director of Administration and Finance will conduct a risk assessment or will supervise an outside entity to perform the risk assessment. The initial risk assessment will seek to reveal the following potential and actual risks to the security and privacy of personal information:

- Unauthorized access of personal information by an employee not entitled to the information.
- Compromised system security as a result of unauthorized access by a third party.
- Interception of personal information during transmission.
- Unauthorized access to paper files containing personal information.
- Unauthorized access to personal information through mobile personal devices, removable media or other means.

The Director of Information Technology and Information Systems and Human Resource Administrator will discuss findings and recommendations resulting from the periodic reviews with relevant Chariho personnel.

The Director of Information Technology and Information Systems and Human Resource Administrator will evaluate Chariho's security practices to determine where improvement is necessary to limit risks, including, but not limited to, ongoing employee training, employee compliance with security policies and procedures, means for detecting and preventing security system failures, and the upgrade of safeguards, if necessary, to limit risks.

IV. Safeguards

In an effort to address the internal and external risks to personal information, Chariho has implemented the following policies and procedures:

A. General Safeguards

Chariho will limit the amount of personal information collected to that necessary to achieve legitimate business goals and to comply with state and federal laws and regulations. Chariho will limit access to personal information to those people with a need to know to accomplish legitimate business goals and to comply with state and federal laws and regulations. Chariho will monitor its security systems for breaches of security.

Upon the occurrence of an incident requiring notification under state law, the Director of Administration and Finance will assemble an Incident Response Team and applicable incident response procedures will be followed. Post-incident review by Chariho following any actual or suspected breach of security and documentation of the actions Chariho takes in response to such breach, including any changes Chariho makes to its business practices relating to the safeguarding of personal information, will be conducted and documented.

Chariho will restrict visitor access where personal information is stored. Visitors will be prohibited from visiting unescorted any area within Chariho's premises that contains personal information.

B. Employee Safeguards

Chariho will post a copy of the Program on the district website. Each employee will participate in employee training about the Program and upon successful completion of the training, certify to attending training and understanding the terms of the Program and the importance of protecting personal information.

Employee training will, among other things, address issues relating to:

- Proper access, use, and disclosure of personal information.
- Proper disposal of personal information.
- Proper safeguards for maintaining, transmitting and storing personal information.
- Logging-off computers.
- Locking files and doors.
- Limiting access to offices.
- Properly handling and protecting mobile devices and removable media.
- Password management.

Employee training will also include training to report any suspicious or confirmed unauthorized access, use or disclosure of personal information, to comply with the Program at all times, and understand that they are subject to disciplinary action for violation of the Program. Employees will be prohibited from storing, accessing or transporting personal information outside the premises of the business, unless in accordance with Chariho policies.

Access to personal information by terminated employees will be revoked as soon as possible following termination and terminated employees will be required to return all personal information in their possession; moreover, all passwords to computer systems will be promptly disabled, all access to electronic files, physical files, email, voicemail and internet access will be promptly blocked, all keys will be surrendered and all forms of identification that permit access to Chariho's premises or information will be returned. Terminated employees will, as a condition of severance, be required to execute an agreement whereby they agree to honor all obligations with respect to maintaining the confidentiality of personal information handled during the course of their employment, to the extent not already contractually bound to do so.

C. Non-Electronic File Safeguards

All tangible files containing personal information will be in a locked room or cabinet or stored securely offsite. The Chariho Regional School District Administrative Team will control the distribution of the keys and will keep track of the number of keys issued. Chariho will limit access to offsite storage facilities containing personal information to those employees with a need to access the files, and Chariho will periodically request an access log to monitor who is accessing such files. When sending personal information via carrier, Chariho will use overnight carriers with tracking and, if sending electronic information, encrypt the information to the extent technically feasible.

D. Electronic File Safeguards

Access to all electronic files maintained on Chariho's servers or Chariho's hardware that contain personal information will be limited to those employees with a need to know.

Moreover, Chariho understands that the following protocols further protect personal information in electronic form. Chariho will, to the extent technically feasible:

- Secure the services of a contract consultant or with internal resources, annually run intrusion testing.
- Install firewall protection and operating system patches on all computers with personal information.
- Install up-to-date versions of security agency software.
- Encrypt personal information that is transmitted across public networks.
- Encrypt all personal information stored on a laptop or other mobile or removable device.
- Limit access to the computer system using complex logins and alphanumeric passwords that require changing periodically and require passwords and limited access to e-files containing personal information.
- Require re-logging after passage of inactive time.
- Prohibit posting or sharing of passwords by employees.
- Lock users out after (3) failed log-in attempts.
- Check websites and software vendor websites for alerts about new problems and implement such vendor approved patches as soon as practical.
- Maintain control of user IDs and other identifiers.
- Maintain passwords in a location and/or format that does not compromise the security of the data the password protects.

- Prohibit the continued use of default passwords by employees (i.e. force employee to change passwords).
- Maintain a reasonably secure method of assigning and selecting passwords or the user of unique identifier technologies such as biometric s or security tokens.
- Terminate any access to personal information by terminated employees.
- Use secure computer and Internet user authentication protocols (i.e. control of user identifications and other identifiers).

E. Third-Party Vendors

When using third-party vendors for services that necessitate the sharing of personal information, Chariho will:

- Obtain, when possible and practical, a copy of the third-party vendor's written information security program designed to comply with the Regulations.

- Require a written contract that the Third-Party Vendor implement and maintain privacy and security measures appropriate to the size and scope of the organization; describes the nature of the information; the purpose for which the information was collected; and a Written Information Security Program by the third-party vendor that complies with R.I.G.L. § 11-49.3-1 et. seq.

F. Disposal

When disposing of files containing personal information, Chariho will follow its policy and records retention schedule, (if applicable) which will include:

1. Shredding all hardcopies of files containing personal information when such information is no longer required or needed to be maintained by Chariho,

2. Destroying all electronic files containing personal information when such information is no longer required or needed to be maintained by Chariho, including the destruction of residual electronic data on computers and other electronic devices.

V. NOTIFICATION OF BREACH

Upon confirmation of any disclosure of personal information or any breach of the security of the safeguards or information system that poses a significant risk of identity theft or disclosure of personal information to an unauthorized person notice shall be given as follows:

A. Notification Procedure

Notification shall be made in the most expedient time possible, but no later than forty-five (45) calendar days after confirmation of the breach and the ability to ascertain the information required to fulfill the notice requirements contained below. In the event that more than 500 Rhode Island residents are to be notified, the school shall notify the Attorney General and the major credit reporting agencies as to the timing, content, and distribution of the notices and the approximate number of affected individuals.

A notification may be delayed if a federal, state, or local law enforcement agency determines that the notification will impede a criminal investigation.

B. Notification Requirements

The Notification shall contain:

a. A general and brief description of the incident, including how the security breach occurred and the number of affected individuals;

b. The type of information that was subject to the breach;

c. Date of breach, estimated date of breach, or the date range within which the breach occurred;

d. Date that the breach was discovered;

e. A clear and concise description of any remediation services offered to affected individuals including toll free numbers and websites to contact: (i) The credit reporting agencies; (ii) Remediation service providers; (iii) The Attorney General; and

f. A clear and concise description of the consumer's ability to file or obtain a police report; how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.

Adopted and effective 2-9-21

PERSONNEL MANAGEMENT SYSTEM

The Basic Education Program (BEP) requires that local educational agencies set policies for the recruitment, hiring, and retention of school staff. These policies must identify student learning as the basis for personnel decision-making. The Chariho Regional School District is dedicated to the concept that there is no more important influence on student learning than the presence of a highly effective educator.

Selection of Certified and Support Staff

When no internal candidates exist for vacancies created by the termination of employment or the establishment of a new position, the position shall be publicly advertised for a period not shorter than five (5) days. The position shall be advertised within five (5) days of the availability of a position or within five (5) days of the passage of the annual budget, as appropriate; nothing herein prohibits the recruitment of qualified candidates. Candidate applications shall be centrally screened for completeness and certification or licensure readiness in accord with the criteria noted in the advertisement and RI Dept. of Education requirements and shall be forwarded to the appropriate administrator.

For certified and educational support staff positions assigned to a single school building, other than those positions discussed elsewhere in this policy, the candidates' applications shall be forwarded to that school building's principal. Once in receipt of all candidates' applications the Principal, in consultation with the School Improvement Team, shall establish an interview team which shall include members of the school community related to the vacancy. The interview team will identify certified and educational support staff candidates who will be offered an interview opportunity. After the interviews are complete and after consultation with the interview team the Principal will recommend a highly qualified candidate for the vacant position to the Superintendent, who shall conduct a second interview and provide the School Committee with the names and related position of those appointed candidates. Educational support staff may be interviewed and recommended to the Superintendent by his or her designee, with the Superintendent making an appointment of a qualified candidate.

Candidate applications for positions assigned to multiple buildings and positions reporting to the Assistant Superintendent, Director of Special Education, Director of Buildings and Grounds, Athletic Director, Director of Educational Technology and Information, or positions for non-athletic extracurricular vacancies (e.g. clubs, curriculum, tutoring) shall be forwarded to the administration responsible for such department or, if no such department exists, the Superintendent of Schools or his or her designee. Upon receipt the appropriate administrator will conduct a search and provide a recommendation to the Superintendent, who will then act accordingly.

Selection of Administrative Staff

The Superintendent shall assemble a search committee, which shall include members of the school community related to the vacancy; it shall also include an invitation to participate to one less member than 50% of the number of members on the School Committee. The search committee shall receive training. Recommendations shall be made in accord with R.I.G.L.:

Education Accountability Act. The search committee will recommend a highly qualified candidate for the vacant position to the Superintendent who shall conduct a second interview and provide the School Committee with the names and related position of those appointed candidates. School Improvement Team members shall be invited to serve on the search committee for building-based administrative positions.

Interview Process

All deliberations of the interview team or search committee, in employment matters, shall remain confidential. The interview team or search committee must consider, but is not limited to, a review of college transcripts, previous evaluations, relevant experience, and reference and background checks, along with other components of this policy. All candidates for teaching positions must conduct a live lesson or, as an alternative, present a teaching video for review by the interview team. Residents of Charlestown, Richmond, and Hopkinton will be provided with an interview opportunity for vacant positions unless they have been previously interviewed within one year by the lead administrator or unless they are disqualified related to another matter noted in this policy.

The District will accept employment applications from relatives of employees, but will not hire said relative if (1) one relative would supervise or could potentially discipline another, (2) one relative would audit the work of another, (3) the relative and the employee or the relative and the District would be in conflict, or (4) if the hiring of the relative would result in a conflict of interest with existing vendors of the District.

If necessary, or otherwise required by this policy, the Superintendent and/or Assistant Superintendent will conduct a second interview. The Superintendent will confirm the recommendation of the interview team or search committee with an appointment of all individuals recommended for certified vacancies. The appointment of individuals recommended shall be conditioned upon criminal background investigations and other requirements including, but not limited to, the completion of IRS forms, RI Department of Health requirements, certification or licensure, transcripts, and statements of service.

Employee Background Screening

In accord with R.I.G.L. 16-2-18.1, prior to the first day of actual work, all prospective employees must agree to a national and state criminal background check with the cost paid by the prospective employee. All offers of employment are conditional upon receipt of a screen with no disqualifying information. Any prospective employee who submits false information shall be terminated.

Current employees, who are convicted of disqualifying offenses as defined in R.I.G.L. 23-17-37, shall be subject to termination. Any employee who is charged with felonious criminal conduct shall notify the Superintendent of said charges within forty-eight (48) hours of the filing of said charge. Failure to report will result in disciplinary action, up to and including termination of employment.

Reassignment, Lay Off, and Recall of Certified and Support Staff

The reassignment, lay off and recall of certified and support staff becomes necessary for a variety of reasons including, but not limited to, the needs of students, changes in enrollment,

and budgetary constraints. When reassigning, laying off, and recalling certified and support staff, consideration shall be given to certification or licensure, performance and experience. Only certified staff of secondary core academic subjects (English language arts, mathematics, science, social studies) and kindergarten through grade four classroom teachers shall be assigned to buildings; all others shall be considered District employees. The Superintendent (or designee) has administrative responsibility for the reassignment of staff. No employee of the District is permitted to work in a position where his/her supervisor or supervisor's supervisor is a relative (father, mother, brother, sister, husband, wife, son, daughter, grandfather, grandmother, grandson, granddaughter); this does not apply to personnel decisions made before July 1, 1997.

Termination of Employment

The District shall be adequately noticed (two weeks for support staff and four weeks for certified staff) when employees voluntarily terminate employment; all District-supplied equipment shall be returned to the employee's supervisor. A Principal may recommend to the Superintendent the termination of any teachers, athletic coaches, instructional or administrative aides, and other personnel assigned to his or her particular school building in accordance with applicable state law, school policy, and any applicable collective bargaining agreements. The Superintendent may seek termination of a certified employee to the extent permitted by Title 16 and any other agreement to which the employee is subject. Said certified or support staff may file an appeal of the Superintendent's decision in accord with the Appeals Policy; nothing herein interferes with the rights of employees to exercise rights under the appropriate collective bargaining agreement.

Exit Interviews

Any employee of the Chariho Regional School District who leaves a position for reasons other than termination or resignation in lieu of termination will be invited to complete an exit survey. Upon return of the completed survey, an invitation will be extended by the Superintendent for the former employee to participate in an exit interview with a subcommittee of the Chariho Regional School District Committee.

Retention of Highly Effective Personnel

The Chariho Regional School District Committee, as a result of its desire to maintain a staff of highly effective certified and support staff, shall recognize high-level performance in a variety of ways. The Committee shall strive to maintain a regionally competitive compensation system. A data-driven and differentiated program supporting the professional learning of personnel shall be provided. All staff shall be evaluated on a regular basis so as to provide relevant and meaningful performance feedback.

Special Education Staffing

The Chariho Regional School District is committed to providing a high quality education for all students. The District recognizes that students with disabilities must be provided with specialized support to achieve at high levels.

A key element in the provision of FAPE (Free Appropriate Public Education) for students with disabilities is the availability of highly qualified teachers, related service personnel, and support

staff to implement each student's IEP (Individual Education Plan). It is also important that said staff engages in a professional development program focused on state and federal regulations and research-based best practice designed to assist disabled students in meeting the goals of their Plans.

The Chariho Regional School District special education staffing plan will be guided by the following:

1. Appropriate personnel must be available to deliver services required by Individual Education Plans.
2. A Free Appropriate Public Education must be delivered in the least restrictive environment.
3. All students must be provided access to the regular curriculum, as appropriate.
4. The goals of the IEP must drive the need for specialized instruction.
5. A full continuum of special education and related services must be available to students, as necessary.
6. Special education staffing decisions will be determined based upon the services identified via the IEP process.
7. Special education staffing must be flexible so as to address the changing needs and numbers of students who require specially designed instruction, related services and individualized interventions.
8. Requests for increases in staffing must be approved by the School Committee.
9. Special education staffing must be in compliance with applicable state and federal law, regulations, and related policies.

The Chariho Regional School District will strive to improve the quality of education for all students and is dedicated to assess and evaluate the delivery of services to students with disabilities.

Non-Fraternization

Sexual relationships, contact, and communications between employees and students are prohibited. Prohibited behaviors include, but are not limited to, flirting and bantering with sexual overtones, dating, courting, engaging in personal relationships that are sexually motivated or unwanted, sexual contact or sexual intercourse. This prohibition applies on and off school property and to students of the same or opposite sex regardless of whether the student or staff member initiates or welcomes the overture. Violations will result in disciplinary action, which may include termination of employment. Sexual misconduct training, with documented participation, is required on a yearly basis.

Hiring for Extra-Curricular and Athletic Activities

When positions become available due to resignations, terminations of service, or a new position established by the School Committee, the vacancy shall be publicly advertised for a period not shorter than five (5) school days. At the discretion of the Superintendent, positions available due to completion of term of employment may be advertised or offered to current, successful personnel in said positions. Members of NEA Chariho Educational Support Professionals are not eligible for these positions, unless specifically and annually approved by the Superintendent of Schools. Following screening and interviews by appropriate personnel and a subsequent recommendation to the Human Resources Administrator, the Superintendent

of Schools will confirm the recommendation and provide the Chariho Regional School District Committee with the names and related position of those appointed candidates. Staff shall be evaluated on a regular basis.

Substitute Staff Procedures

Substitute personnel are required to attend orientation or training session(s). All personnel and substitutes, with the exception of those assigned to second shift, are required to use the District's designated substitute management system. Substitutes may be removed by the Human Resources Administrator for reasons that include, but are not limited to, failure to follow policy and procedures, attendance, and performance.

Substitute teachers, no longer certified by the Rhode Island Department of Education, will be authorized to teach in the District upon receipt of (1) original transcripts from an accredited postsecondary institution indicating date of Bachelor's Degree, (2) completed application and required related employment documents, and (3) federal background investigation. Authorization to substitute is contingent upon a review of said documents.

Substitute teachers are responsible for planning, instruction, assessment, grading, and other typical teaching responsibilities. The daily rate for substitutes for certified employees shall be ~~$85.00~~ $120.00. ~~except that the daily rate for retired teachers shall be $90.00. A substitute who serves for thirty (30) or more consecutive school days in the same assignment without undocumented absence will be compensated at $40.00 above said daily rate; payment will not be retroactive.~~ Commencing on the 135th day of substitute service in Chariho in the same school year, substitute teachers will be compensated in accord with the following schedule; payment will not be retroactive.

*Years of Substitute Service	Daily Rate
1	$170.00
2	$175.00
3	$180.00
4	$185.00
5	$190.00
6	$195.00
7	$200.00
8	$205.00
9	$210.00
10	$215.00

*Year must equal at least 135 days of service. Statements of service for prior years of service must be provided, in writing, to the Human Resources Administrator by October 1 of each year.

The Superintendent is authorized to adjust the above daily rates for certified substitute teachers when a position is difficult to fill by increasing those rates by up to 50%. Substitutes for school nurse teachers will be compensated at $36.00 per hour.

The hourly rate for substitutes for personnel represented by NEA Chariho Educational Support Professionals shall be 85% of the probationary rate, as defined in Appendix A of the collective bargaining agreement. When said rate falls below the minimum range, the probationary rate shall be utilized

No substitute may work more than twenty-eight (28) hours per week, except as approved by the Superintendent of Schools for long-term substitute assignments. This guideline shall not apply to retired teachers, except that they shall be limited to a total of ninety (90) days per school year. Substitutes for certified employees who are also part-time employees (stipend, salary or hourly) and/or coaches of the Chariho Regional School District may substitute for the District for no more than eight (8) hours per week.

The following Memorandum of Agreement precludes a long-term substitute, who is in a position created by a leave, from becoming a member of the bargaining unit, thereby eliminating the issues of recall rights, benefits and unemployment compensation. "Effective this date (2/27/96), the fact that a substitute teacher has worked a total of one hundred thirty-five (135) or more days in any school year does not, in itself, require the employment of the substitute teacher by the Chariho Regional School District, or shall such substitute teacher be deemed to be a member of the bargaining unit or entitled to any of the benefits of the agreement between the Chariho Regional School District Committee and NEA Chariho, solely by reason of having worked one hundred thirty-five (135) or more days in any school year." These substitutes will receive proper notification of completion of assignment. Substitutes will not be entitled to unemployment benefits during the summer recess because they have a reasonable reassurance of re-employment when school resumes.

Substitutes who are eligible for health care benefits through the Employer Shared Responsibility section of the Patient Protection and Affordable Care Act are required to have their copayment for healthcare benefits deducted from their bi-weekly paychecks. The co-pay on an individual plan is limited to 9.5% of the substitutes W-2 wages during the stability period. Should the employee choose to cover their dependents (other than spouse) under a family plan, the entire difference between a family plan premium and an individual plan premium will also be deducted from the bi-weekly paychecks. At the end of the calendar year, the District will calculate any balance due for a co-pay on an individual plan and/or any balance due for the difference between an individual and family plan. Substitutes are required to notify the Human Resources Administrator of any error in related calculations within five (5) school days of the error.

Substitutes will be evaluated on a regular basis.

Adopted and effective 8-20-13, Revised and effective 9-10-13, 11-18-14, 3-24-15, Revised and effective 7-14-15, Revised 4-12-16-Effective 7-1-16, Revised and effective 3-16-17; Revised and effective 1-22-19; Revised and effective 2-11-20; Revised 2-9-21; Effective 7-1-21

Responsible Use of Technology Policy

Purpose and Expectations

The Chariho Regional School District ("District") uses technology as one tool to support our mission of ensuring that all students meet high academic standards and are prepared for lifelong learning and productive global citizenship. The District supports the notion that students and educators should have ready access to the vast instructional potential of technological tools.

The District's Responsible Use of Technology Policy (RUTP) provides guidance to students ("users") and District employees ("providers") in the responsible use of technology for educational purposes, research and communication. This policy provides guidelines but does not attempt to state all permitted or prohibited activities. The District has the right to prohibit any District technology use by providers and users not stated in this policy.

Every user needs technology skills and knowledge to succeed as an effective and productive citizen. Every provider needs access to technological tools to provide users with the best possible opportunity for success. The 21st century learning environment includes all types of resources including computing devices, Internet sites and software. Users and providers have access to personal technology including, but not limited to, computers and cell phones and District technology which includes local network resources, Internet service, and a variety of digital devices including, but not limited to, laptops, tablets, desktop computers, smart boards and software. All use of District technology is intended to support the effective implementation of the Chariho Regional School District's curriculum, standards and business requirements.

Only educational software and digital tools approved by the District may be used for instructional purposes.

Internet Safety, CIPA and Personal Use

The District complies with the Children's Internet Protection Act ("CIPA"). The District uses technology protection measures to block or filter, to the extent practicable, access to content or transmission of visual depictions, communications or otherwise, that are obscene, pornographic, and harmful to minors over the network. Providers, even when they allow access for educational reasons to sites normally blocked or filtered, also provide reasonable monitoring of users Internet use. It is the responsibility of all to monitor his/her own access and use sound judgment in matters related to potentially obscene, pornographic, and/or harmful materials. The District's content filter will be frequently updated and be active when any District device is used outside of school and when any personal device accesses the Internet via the District's network.

This policy applies regardless of whether such use occurs on or off school property and it applies to all District technological resources including, but not limited to, computer networks and connections; the resources, tools, and learning environments made available by or on the network; and all devices that connect to those networks. When issued a mobile computing device by the District, users and providers may use it at school or at home. The District permits personal use so long as it occurs on personal time, complies with this policy and CIPA. Personal use should not interfere with District activities and other established policies and procedures. Users and providers are responsible for their actions and activities involving District technology, networks, and Internet services and for keeping their files, passwords, and accounts secure. Users and providers accessing the Internet via District technology assume personal responsibility and liability, both civil and criminal, for uses of the Internet not authorized by the policy or accompanying guidelines. Damage, malfunction, theft, or similar event to an issued and assigned device must be reported within twenty-four (24) hours of the event.

Unauthorized Software and Hardware Modifications

Providers and users shall not install software or hardware on the District-issued devices that can monitor or record the Internet activity, access the files or electronic communications, or capture any data transmissions from other District or non-District-issued equipment. Additionally, hardware installation, repairs, and hardware configuration of the District-issued devices will be performed by the District IT staff or by authorized users or providers under the direct supervision and responsibility of District IT staff. All District technology, which includes software, is subject to District IT oversight and control.

Social Media

Personal or private use of social media may have unintended consequences. Social media is defined as Internet-based applications including, but not limited to, Facebook, Twitter, chat rooms, instant messaging, blogs, wiki's, etc., that turn communication into interactive online dialogue.

With regard to Providers, postings to social media should be done in a manner sensitive to the providers' professional responsibilities and should maintain an appropriate professional relationship with users. The District authorizes providers to access social media from the District's network provided such access has an educational purpose.

With regard to Users, social media may not be used in a way that undermines the District's mission or causes a substantial disruption to the school environment. Providers and Users are also bound by other Chariho policies, such as the Personnel Management System Policy and the Standards for Student Behavior Policy.

Personal access and use of social media from the District's network and Internet service by users and providers is prohibited during instructional time, unless specifically intended for educational purposes.

All use of technology resources, including accessing social media with District property or during school-sanctioned events, shall be in accordance with all provisions of this policy.

No Expectation of Privacy with District Technology, Networks, or Internet Services

The District retains control, custody and supervision of all technology, networks and Internet services owned or financed by the District. The District reserves the right to monitor all usage including Internet usage of the District-issued equipment. Users and providers shall have no expectation of privacy with regard to the use of District technology and District property including network, Internet access or files and email. No expectation of privacy extends to all files stored on the District-issued device including email and Internet usage of the device.

The District reserves the right to monitor users' and providers' online activities accessed through District technology, including networks or Internet services. The District can access, review, copy, store or delete any electronic communication or files and disclose them to parents, guardians, teachers, administrators or law enforcement authorities as the District deems necessary or mandated by law.

The District will not make use of any camera or microphone on District technology for remote monitoring purposes except during distance learning. The District can monitor devices not issued by the District that are using the District network or Internet services.

Other Guidelines for Users

A. Technology Use is at the Discretion of the District

Use of District technology, networks and Internet services can be restricted or prohibited. Users must also follow this policy when using allowable personal digital devices including, but not limited to, laptop computers, tablets and cell phones while on District property, at school activities and/or riding District-provided transportation.

B. Responsible Use

1. Users are expected to use District technology primarily for educational purposes.
2. Users are expected to comply with this policy and when using technology outlined in this policy.
3. Users are responsible for their actions and activities involving District technology, networks and Internet services and for keeping their files, passwords and accounts secure.
4. Users shall not use personal devices during instructional time without permission.
5. Users should promptly inform their teacher or school administrator if they are aware of any technology issue that is contrary to this policy.
6. Users are expected to comply with any District requests to limit use of the District technology.

C. Prohibited Uses

While technology can be a valuable resource in an academic setting, it has the potential for misuse. Prohibited use will result in disciplinary action as defined by the appropriate Standards for Student Behavior Policy and other applicable policies and may also include loss of use of District technology.

1. Inappropriate Material: Accessing, submitting, posting, publishing, forwarding, downloading, scanning or displaying materials that are defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing and/or illegal.
2. Illegal Activities: Using District technology, networks and/or Internet services for any illegal activity or activity that violates other District policies, procedures and/or school rules.
3. Violation of Copyrights: Copying or downloading copyrighted materials without the owner's permission or any other activity that violates other District policies regarding copyrighted material.
4. Non-School-Related Uses: Using District technology, networks or Internet services for private financial gain, commercial, political, religious, advertising or solicitation purposes is prohibited.
5. Misuse of Passwords/Unauthorized Access: Sharing passwords, using other users' passwords without permission and/or accessing other users' accounts or providers' accounts.
6. Malicious Use/Vandalism: Any malicious use, disruption or harm to District technology, including, but not limited to, modifying or uninstalling device configurations, hacking activities and creation/uploading of computer viruses. Vandalism includes damaging computer equipment, files, data or the network in any way.
7. Unauthorized Access of Electronic Communication Tools: Accessing resources such as email, chat, social networking sites, texting and telephone services without specific authorization from instructional staff.

D. Personalization of Issued and Assigned Devices

1. Users are allowed to personalize devices within the parameters of this policy. Personalization must not impede the instructional and educational use of the device and may not be any form of non-digital customization including, but not limited to, stickers, decals or artwork.
2. Users are not allowed to make configuration changes that may interfere with maintenance, software installation, or software upgrades.
3. Personalization must conform to all other applicable policies of the District. No use of media prohibited by other policies is allowed.
4. The District assumes no liability or responsibility for personal electronic property saved to a device. This includes, but is not limited to, personal software, files, games, eBooks, and other media.
5. The District assumes no liability or responsibility for unauthorized charges made by users that may include, but are not limited to, credit card charges, long distance telephone charges, and electronic payment services.
6. In the event that device internal memory is insufficient for the download or use of required educational content, the provider will be required to remove personal files.

E. Communication of Policy

This policy shall be provided to all users and parents/guardians on an annual basis. All users shall be provided with instruction regarding this policy.

Other Guidelines for Providers

A. Primary Intent

District technology is made available to providers to allow for the enhancement, enrichment, and expansion of educational opportunities for users. Its primary use is for educational purposes.

B. Responsible Use

1. Providers are expected to use District technology primarily for educational purposes.
2. Providers are expected to comply with this policy and when using technology outlined in this policy.
3. Providers are responsible for their actions and activities involving District technology which includes networks and Internet services, and for keeping their files, passwords and accounts secure.
4. Providers should promptly inform District IT staff or school administration if they are aware of any technology use or issue that is contrary to this policy.
5. Providers are expected to comply with any District requests to limit use of District technology.
6. Providers should understand that they are held to a higher standard than the general public and are expected to set the example with regard to policy adherence, standards of conduct and ethics. Reference should be made to other Chariho policies, including the Personnel Management System Policy.

C. Prohibited Uses

1. Inappropriate Material: Accessing, submitting, posting, publishing, forwarding, downloading, scanning or displaying materials that are defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing and/or illegal.

2. Illegal Activities: Using District technology, networks and/or Internet services for illegal activity or activity that violates other District policies, procedures, and/or school rules.
3. Violation of Copyrights: Copying or downloading copyrighted materials without the owner's permission or any other activity that violates other District policies regarding copyrighted material. Under no circumstance may software purchased by the District be copied or distributed.
4. Non-School-Related Uses: Using District technology, including networks or Internet services for private financial gain, commercial, political, religious, advertising or solicitation purposes is prohibited.
5. Misuse of Passwords/Unauthorized Access: Sharing passwords, using other providers' passwords without permission and/or accessing other providers' or users' accounts.

D. Personalization of Issued and Assigned Devices

1. Providers are allowed to personalize devices within the parameters of this policy. Personalization must not impede the instructional and educational use of the device.
2. Providers are not allowed to make configuration changes that may interfere with maintenance, software installation, or software upgrades.
3. Personalization must conform to all other applicable policies of the District. No use of media prohibited by other policies is allowed.
4. The District assumes no liability or responsibility for personal electronic property saved to a device. This includes, but is not limited to, personal software, files, games, eBooks, and other media.
5. The District assumes no liability or responsibility for unauthorized charges made by providers that may include, but are not limited to, credit card charges, long distance telephone charges, and electronic payment services.
6. In the event that device internal memory is insufficient for the download or use of required educational content, the provider will be required to remove personal files.

E. Communication of Policy

All providers shall be given instruction regarding this policy.

Revised 7-17-12-effective 8-29-12; Revised 7-16-13-effective 9-1-13; Revised and effective 12-16-14; Revised 5-12-15-effective 7-1-15; Revised and Effective 2-9-21