Highland Local Schools
Data Governance Guidelines

Introduction

The Highland Local School District views the privacy and security of both student and staff information as a priority and an important responsibility. The district collects, creates and stores confidential information on students, parents/guardians, employees and applicants for employment which by law need to be kept confidential.

In order for the District to accomplish this, and for our data governance program to be effective, we must ensure personnel, policies, procedures and organizational structures are in place to make data accurate, consistent and secure.

The purpose of the Data Governance Guidelines is to institute effective data governance by establishing accountability, ensuring that the district's data is accurate, accessible and protected, and by establishing responsibility along with procedures to be used for the management and protection of information.

The Highland Local School District is committed to not only maintaining strong privacy and security protections but also ensuring that the rules and principles of data protection are followed.

Overview

It is Highland Local School's policy that all forms of data and information are protected from unauthorized disclosure, change, or destruction throughout it's life cycle, either accidental or intentional. The life cycle being: Identifying the need; Acquiring and Creating; Managing and Storing; Protecting; Using and Sharing; and the Archiving and Deleting of information.

The protection of information in all forms includes levels of security over equipment, software and practices used to process, store and transmit data and/or information. A high level of personal responsibility is expected of all users with access to the district's technology resources. District system users shall sign the HLS Staff/Student Computer and Internet Acceptable Use Agreement/Contract before accessing any district technical system.

The Highland School's data policies and procedures will be made available to individuals responsible for their implementation and compliance. All data governance policies and procedures will be reviewed annually by the Data Governance Committee.

Scope and Regulations

Highland's Data Governance policies, standards, processes and procedures apply to all staff as well as students, employees, volunteers who have access to do the district's data, contractual third parties and agents of the district.

Data and information include but are not limited to:

A. Speech - face to face or communications by phone or any current and/or future technologies
B. Hard copy data
C. Communications sent by post/courier, fax, email, text, chat or any social media
D. Data stored and/or processed by any electronic device (servers, computers, tablets, mobile devices)
E. Data stored on internal, external or removable media or cloud based services.

To help control the safeguarding of confidentiality data classifications are used.

(PII) Personally Identifiable Information -

Any information that can be used to distinguish or trace an individual's identity such as name, SSN, birthday, mother's maiden name. Also, any information that is linkable to an individual such as medical, educational, financial and employment information.

Confidential Information-

Private information that is sensitive in nature. For example: student records, personnel information, financial information and system access password.

Internal Information-

Information intended for unrestricted use within the district. Unauthorized disclosure of this kind of information may not be appropriate due to copyright, legal or contractual services.

Directory Information-

Information contained in an education record that would not be considered harmful or an invasion of privacy if disclosed. (ei: student's name; date and place of birth; parents' names; grade level; enrollment status; participation in district sponsored/recognized activities/sports, etc.)

Public Information-

Information that has been approved for public release such as mailings.

Highland Local School District will abide by any applicable regulatory acts including, but not limited to:

(CIPA) Children's Internet Protection Act

CIPA requires districts to put measures in place to filter Internet access and other measures to protect students.
http://www.fcc.gov/guides/childrens-internet-protection-act

(COPPA) Children's Online Privacy Protection Act

COPPA puts special restrictions on software companies about the information they can collect about students under 13. So, students under 13 can't make their own accounts, teachers have to make the accounts for them. In making the accounts, teachers need to be aware of their responsibility under FERPA.
http://www.coppa.org/

(FERPA) Family Educational Rights and Privacy Act

FERPA requires that schools have written permission from the parent or guardian in order to release any information from a student's education record. So the most important thing is that, with some very specific exceptions, you shouldn't be sharing student information with apps and websites without parent permission.
http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

(HIPPA) Health Insurance Portability and Accountability Act

Used to measure and improve the security of health information.
http://www.hhs.gov/ocr/privacy/hipaa/understanding/

(PCI DSS) Payment Card Industry Data Security Standard

This covers the management of payment card data.
http://www.pcisecuritystandards.org/

(PPRA) Protection of Pupil Rights Amendment

Gives parents and minor students' rights regarding surveys, collection and use of information for marketing purposes, and certain physical exams.
http://www2.ed.gov/policy/gen/guid/fpco/ppra/index.html

Compliance

All Highland Local School District staff are to be good stewards of data. They are responsible for the security and integrity of their data and are expected to treat data security responsibly. PII, confidential information and internal information shall be stored so that it is inaccessible to unauthorized individuals. The downloading and uploading or transferring of PII, confidential information and internal information shall be strictly controlled. When printing staff will use secure printing. Materials should never be printed indiscriminately or left unattended. Employees shall be aware of their surroundings and should never discuss PII or confidential information in public areas if the information can be overheard. This includes the use of cellular telephones in public areas.

Any user (employees, contractors, agents) will notify their supervisor immediately if PII has been disclosed. The supervisor will then immediately notify the Data Breach Response Team.

Any violation of district policies or procedures by employees, staff, volunteers, and outside affiliates may result in disciplinary action up to and including dismissal or in the case of outside affiliates, termination of the affiliation. Failure to comply with this policy by students may constitute grounds for corrective action in accordance with Highland Local Schools' policies. Additional penalties associated with state and federal laws may apply.

Employees may be disciplined or terminated, and students suspended or expelled, for violating the district's technology policies and procedures. Any attempted violation of the district's technology policies or procedures may result in the same discipline or suspension of privileges whether successful or not.

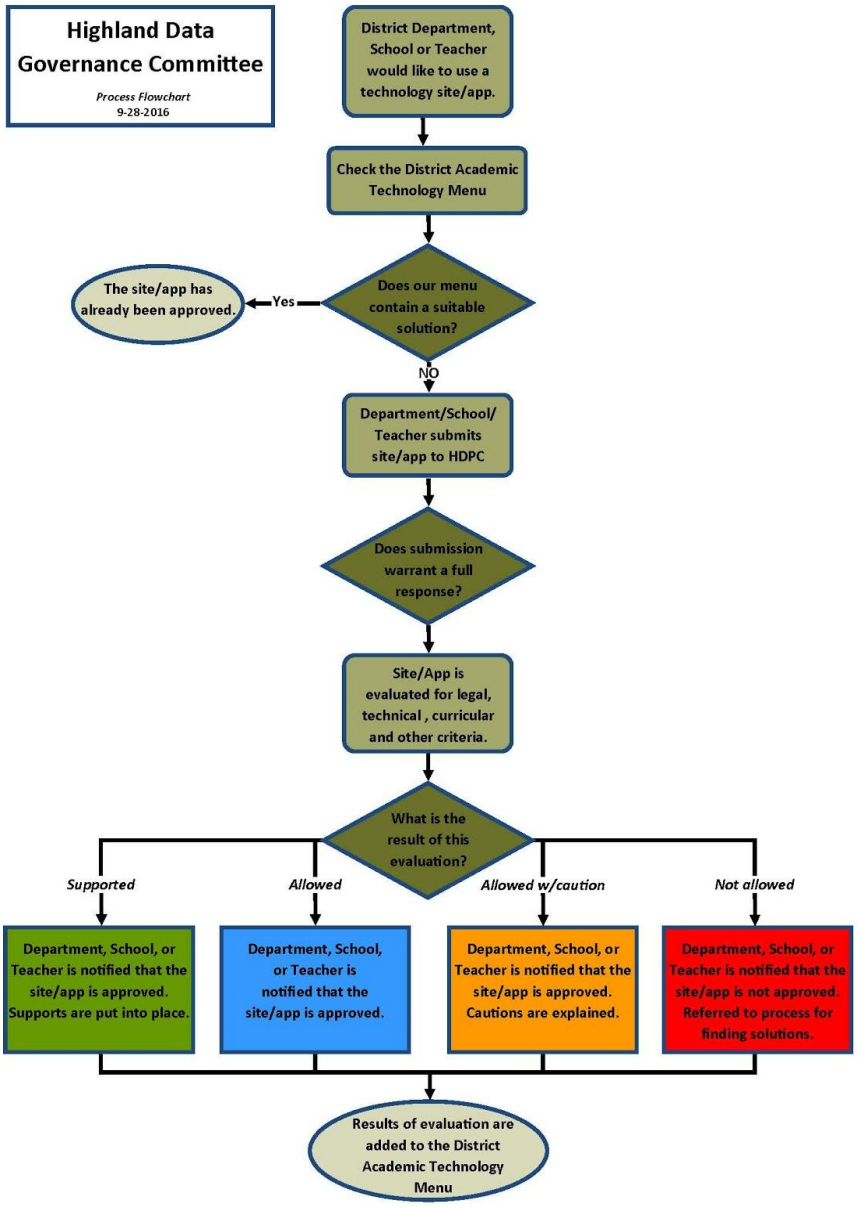
Example violations include:

1. Unauthorized disclosure of PII or Confidential Information.
2. Sharing your user IDs or passwords with others.
   (exception for authorized technology staff for the purpose of support)
3. Applying for a user ID under false pretenses or using another person's ID or password.
4. Unauthorized use of an authorized password to invade student or employee privacy.
5. Installation or use of unlicensed or unvetted software on Highland Local Schools' technological systems.
6. The intentional unauthorized altering, destruction, relocation, or disposal of Highland Local Schools information, data and/or systems. This includes the unauthorized removal or relocation of technological systems such as laptops, internal or external storage, computers, servers, backups or other media, copiers, etc. that contain PII or confidential information.
7. The introduction of computer viruses, hacking tools or other disruptive or destructive programs.

Data Governance Committee/Responsibilities

The Highland Local Schools Data Governance Committee is responsible for ensuring security policies, procedures and standards are in place and adhered to by the district. It is also responsible for reviewing the Data Governance Guidelines annually. This committee meets two times a year with additional meetings being called if necessary. The 2016-17 committee is lead by Roger Saffle, Supervisor of Technology; members are Catherine Aukerman, Superintendent; Laurie Boedicker, Director of Curriculum/Instruction; Paul Gerycz, High School Vice Principal; Rob Henry, Middle School Principal; James Carpenter, Hinckley Elementary School Principal; LeAnn Gausman, Granger Elementary School Principal; Katie Kowza, Sharon Elementary School Principal; Shea Strittmather, High School Teacher; Lisa Reynolds, Middle School Teacher; Hannah Everhart, Elementary School Teacher; Amy Lyon, Elementary School Teacher; Bernadette Yu, Elementary School Teacher; and Ann Marie Platten, Technology Administrative Assistant.

The district has a process in place for the vetting of new digital resources. Staff are required to complete the steps outlined in the Highland Data Governance Committee flowchart below. Which can also be found on the district's website technology page.



This is to ensure that the resource meets a business and/or instructional need, security requirements and that it does not contain malware, viruses or other security risks prior to its use. Once the the digital request form has been submitted the HDGC will evaluate the resource at the next scheduled meeting. The resource will then be categorized as Supported, Approved, Approved with Caution or Denied. If the resource is approved for instructional purposes, there has to be parent notification/approval before the resource can be used in the classroom. Under no circumstances can staff act as a parental agent when creating student accounts for online resources. *Only approved district resources are to be used.*

A list of evaluated software in use is maintained on the Technology site. A complete list of all vetted software can be found in the staff portal. It is the responsibility of the staff to submit a review request if a resource is not listed. If a resource is denied or has not yet been reviewed it is not allowed to be used on district devices, as part of district business or for instructional purposes. Again, if the resource is approved for instructional purposes, there has to be parent notification/approval before the resource can be used in the classroom.

Data Management

Data Management is the development and execution of procedures that ensure the accuracy and security of data. This includes ensuring that account creation and data access guidelines match employee job functions. Staff is to be trained in the district's data security policies and all data is to be tracked accurately. Reviews are to be made on all employees with custom data access. Contracts with software providers are to be reviewed as well making sure they are current and meet data security standards.

Staff is responsible for securing the transmission of sensitive data. Secure data transfer protocol is be in place for the regular transmission of student data to approved services. Passwords should never be included in any communications and files that are classified, confidential or restricted should never be transmitted through email or to third parties without approval. Transmission of student data to services such as a learning management systems will be managed by the technology department using a secure data transfer protocol, e.g. SFTP or FTPS instead of unsecured FTP.

The transfer of documents labeled classified, confidential or restricted to any personal storage device (external hard drives, USB drives, memory cards, rewritable CD/DVDs, laptops, cloud storage) is not permitted. When staff are no longer employed by the district any data in their possession is to be deleted or destroyed. All technology equipment is to be returned to the district.

Data Security

District Data Security shall be checked regularly for any threats that could affect the management and protection of information. This security applies to all forms of data - data stored on devices as well as "cloud storage". All users must ensure that they are securely storing their data whether through their mapped folders or on remote server storage provided with their Google Drive accounts. Remote access into the Highland Schools' network from outside is allowed through the staff/student portals with the expectation that the same level of protection will be applied to all PII, confidential information and/or internal information accessed remotely as information stored and accessed within the Highland Schools' network. Outside vendors and contractors needing outside network access must do so by VPN. All other network access options are prohibited.

When sharing files, staff must follow all policies and procedures regarding professional conduct and communication. They must also ensure that the other users accessing the information have the appropriate access rights to the information based on their job function. Files should be shared on an as needed basis only. Staff are

prohibited from copying content that contains confidential information, student records or district created curricular or operational documentation, files, or data. Attempting to gain or gaining unauthorized access to files or the cloud storage of another is prohibited. As with other forms of district technology, district employees, students, and other Google Suite for Education drive users have no expectation of privacy on data stored on this platform.

A reminder of Highland's Records Retention Schedule and shredding guidelines should be made at the beginning of each school year. The Technology Supervisor will regularly review systems and data to ensure that data that is no longer needed is destroyed. Student's personal folders will be maintained for one year after their final date of attendance and employee personal folders will be maintained for 30 days after their final work day, unless it is deemed necessary for district administration to maintain access.

System Security

District employee electronic access to PII confidential information will be given only if it is necessary for the performance of their duties. All user are assigned to a security group, both in Student Information System (SIS) and Active Directory (AD). SIS and AD each have groups with their own established role based permissions for establishing access.

These groups in SIS are: Office Staff, Counselor, Read Only All, District Manager, Staff Full, Administrator, Principal, Power Scheduler, Special Ed, Out of District Teachers, JVS, Bulletin Updater, FinalForms, District PS Admin, and Front Desk - Locate Student Only.

These groups in AD are: PasswordResetters, StaffAll, StaffBOE, StaffGE, StaffHE, StaffHS, StaffMS, StaffPreKTeam, StaffPsychTeam, StaffTech, StudentsGE, StudentsHE, StudentsHS, StudentsMS, and StudentSE.

A new employee notification is sent from the Highland Board Office to the Technology Department after board approval. This notification includes position, building assignment(s), start date and signed AUP and Data Governance Guideline, which will be kept on file in the technology office. It is only after this notification has been received that the Technology Department creates user accounts. When a staff member's employment has ended account permissions are revoked immediately unless directed otherwise by a district administrator.

Active Directory will be used to maintain account security controls. The district will disclose PII confidential information with authorized district contractors/agents and systems access given on an as needed basis only. Verification that contract, terms of service and privacy policies are current and meet district security requirements will be done. All providers are to have adequate data security, proper access controls and password security.

Methods for controlling access to PII, confidential information, internal information and computing resources include identification (user ID) and authorization (access controls). Highland Local Schools require the use of passwords for network access and for access to secure sites and information. Single sign on (SSO) will be used when possible and remote access will be given with the same level of protection. QR badges should be secured by the classroom teacher.

Users are never to share their password(s) with anyone other than a designated security manager. Long-term subs are given their own username/password and access to the Highland Local School District network. Powerschool must be accessed as the teacher of record. In those instances the username/password has to be shared. The Technology Department can unlink a teacher's Powerschool password/account from their email and Google Drive before they share it with a long term sub.

Passwords will be changed yearly and guest passwords will be changed more frequently. When creating a password for secure information it is important not to use passwords that are easily guessed based on user association (children's names, pet names, birthdays, etc.). Passwords cannot contain highland, hornet, password, username or other such common words, or student ID number. The existing password may not be reused when changing the password.

No user will have local administrator permissions. If one is required for specific software/application the technology department is responsible for applying the administrator password. No user will have domain administrative access. This access is limited to technology department technicians and the technicians requiring domain access will have separate accounts for this access. All access permissions will be audited.

Physical Security

Highland's network systems are to be installed/housed in an access-controlled area with controlled temperature and humidity levels. All servers containing PII, confidential and internal information are to be installed/housed in a secured area preventing theft, destruction or unauthorized access. Network systems and equipment are to be properly secured at all times.

District assets will be maintained in the district-approved technology inventory program and verified by a regular inventory verification process. All devices are to be inventoried by the technology department (network appliances, servers, computers, laptops, mobile devices, external hard drives, etc.) There will be a bi-annual inventory verification of staff, classroom and student devices. Technology assets have to be approved by the Technology Supervisor and purchased through the technology department. Failure to have purchases approved will result in one of the following: lack of technical support; device removal from premises; or denied access to technology resources.

Unsecured laptops or removable storage devices will not be used to transport or store sensitive information. Should a requirement exist for sensitive or confidential information to be stored on a laptop or removable media, the device must be encrypted and be physically secured when unattended. Removable media such as USB drives and optical disks (e.g., CD-ROM or DVD-ROM) or personal Cloud storage (e.g. Google Drive, Dropbox, OneDrive, etc) should not be used to transport sensitive or confidential information. Laptops in the District must be secured in a locked office/classroom when unattended for an extended length of time or left overnight.
When laptops are taken out of District, the laptop must be kept under positive control of the owner. It should be in hand, in sight or locked in a secure location at all times. Laptop users are responsible for securing laptops at all times, but especially when traveling.

Computers and other systems are to be secured against unauthorized use. Users should never leave a devise logged in or unattended as this leaves it open to unauthorized use. The delivery and removal of all asset-tagged and/or data-storing technological equipment shall be monitored and controlled. No technology equipment, regardless of how purchased or funded, shall be moved without the knowledge/approval of the Technology Department. The Technology Department is responsible for equipment entering or exiting their assigned location and updating the inventory so that in-school transfers, in-district transfers or location changes are reflected.

The Supervisor of Technology shall approve disposals of any district technology asset. Technological equipment or systems being removed, transferred to another organization or moved to storage shall be appropriately sanitized in accordance with applicable policies and procedures ensuring that PII, confidential or internal information as well as Microsoft licenses or other software licenses are destroyed.

All employees have building access (Board Office issued ID badges and building codes) that are constantly monitored so that only current employees continue to have this access. District-all access permissions will be limited. Employee badges must be worn at all times by Highland staff while on school property. The badge is the property of the school district and must be surrendered to the Highland Board of Education Office upon request.

Virus, Malware, Spyware, Phishing and Spam Protection

Highland Local School desktops, laptops, and file servers are protected using virus/malware/spyware software. All files and systems are scanned. An on-access scan is performed on all “read” files continuously. A full scheduled scan runs monthly on all servers and is performed during non-peak hours. A WSUS server is used to keep all clients up-to-date with Microsoft patches. Servers are patched and rebooted on a monthly basis.

To balance educational Internet resource and app use with student safety and network security, the Internet traffic from all devices that authenticate to the network is routed through iBoss, the district’s firewall and content filter, using the user’s network credentials. This process sets the filtering level appropriately, based on the role of the user (e.g., student, staff, or guest). All personal devices are required to authenticate prior to gaining access to the district network and all devices on the district network is routed through the district firewall and content filter. All sites that are known for malicious software, phishing, spyware, etc. are blocked.

Email for both staff and students is filtered for viruses, phishing, spam and other threats by Google services.

District Training

Highland Local Schools will provide security training to all new staff on technology policies and procedures which include confidentiality and data privacy. Annual training will be given to all staff on federal regulations, confidentiality, technology policies and procedures, the use of digital resources and electronic records. HLS Administration will also receive annual training regarding federal regulations, data privacy and security.

Critical Incident Response

Controls are in place so that the district can recover from damage to or breach of critical systems, data or information. Every school, department or individual is required to report any information immediately to the Superintendent and the Supervisor of Technology so they will know how to respond whether it is a system emergency or some other occurrence (fire, vandalism, system failure, data breach, natural disaster, etc.)

The district will maintain near-line and offsite data backup which allow for full recovery of critical systems in the event of a disaster along with a recovery plan that includes processes so that the district can continue operations and efficiently restore any loss of data.

Highland Local Schools will also maintain a Data Breach Response Plan enabling the district to respond efficiently to an actual or suspected data breach involving PII, confidential or protected information and other significant cybersecurity incidents. This response plan includes processes for validating, containing and analysing the breach so that the scope and composition can be determined and notification can be provided. When a breach occurs the specific handling will be done by the Data Breach Response Team which will be made up of the Superintendent, the Technology Supervisor and the Administrator/Supervisor of the building/area where the breach occurred. This team will then minimize the impact to the staff/students after the breach has occurred and notify the data owners, state/federal agencies and law enforcement as deemed necessary.

Social Media Guidelines

Highland Local Schools recognizes that access to technology in school gives students, parents and teachers greater opportunities to learn, engage, communicate and develop skills that will prepare them for work, life and citizenship. We are committed to helping students develop 21st-century technology and communication skills.

To that end, below are the the guidelines and behaviors that Highland employees are expected to follow when using school technologies or when using personally-owned devices on the school Campuses.

- Employees are expected to follow the same rules for good behavior and respectful conduct online as offline.
- Misuse of social media can result in disciplinary action.
- Highland Local Schools makes a conscious effort to ensure staff and students' safety and security online but will not be held accountable for any harm or damages that result from misuse of social media technologies by Highland employees.

We realize that teachers and staff use social networking/media (Twitter, Facebook, etc.) as a way to connect with others, share educational resources, create and curate educational content and enhance the classroom experience. While social networking is fun and valuable, there are some risks you should keep in mind when using these tools. In the social media world the lines are blurred between what is public or private, personal or professional.

We've created these social networking/media guidelines for you to follow when representing the school in the virtual world.

Please Do The Following

Use Good Judgment

- Highland Schools expects you to use good judgment in all situations.
- Staff must know and follow the school's Acceptable Use Policies and Data Governance Guidelines.
- Regardless of your privacy settings, assume that all of the information you have shared on your social network is public information.

Be Respectful

- Always treat others in a respectful, positive and considerate manner.

Be Responsible and Ethical

- If you are approved to represent the school, unless you are specifically authorized to speak on behalf of the school as a spokesperson, you should state that the views expressed in your postings, etc. are your own. Stick with discussing school-related matters that are within your area of responsibility.
- Be open about your affiliation with the school and the role/position you hold.
- Postings to social media should be done in a manner sensitive to the staff member's professional responsibilities.

Be a Good Listener

- Keep in mind that one of the biggest benefits of social media is that it gives others another way to talk to you, ask questions directly and to share feedback.

- Be responsive to others when conversing online. Provide answers, thank people for their comments, and ask for further feedback, etc.
- Always be doing at least as much listening and responding as you do "talking“.

Do Not Share the Following

Confidential Information

- Do not publish, post or release information that is considered confidential or not public. If it seems confidential, it probably is. Online "conversations" are never private. Do not use your birthdate, address or cell phone number on any public website.

Private and Personal Information

- To ensure your safety, be careful about the type and amount of personal information you provide. Avoid talking about personal schedules or situations.
- NEVER give out or transmit any personal information of students, parents, or co-workers.
- Don't take information you may receive through social networking (such as email addresses, customer names or telephone numbers) and assume it’s the most up-to-date or correct.
- Always respect the privacy of the school community members.

Please Be Cautious With Respect To

Images

- Respect brand, trademark, copyright information and/or images of the school (if applicable).
- You may use photos and video (products, etc.) that are available on the school’s website.
- It is not acceptable to post pictures of students without the expressed written consent of their parents.
- Do not post pictures of others (co-workers, etc.) without their permission.

Other Sites

- A significant part of the interaction on blogs, Twitter, Facebook and other social networks involves passing on interesting content or linking to helpful resources. However, the school is ultimately responsible for any content that is shared. Don't blindly repost a link without looking at the content first.
- Pay attention to the security warnings that pop up on your computer before clicking on unfamiliar links. They actually serve a purpose and protect you and the school.
- When using Twitter, Facebook and other tools, be sure to follow their printed terms and conditions.

If You Make a Mistake

- Be sure to correct any mistake you make immediately, and make it clear what you've done to fix it.
- Apologize for the mistake if the situation warrants it.
- If it's a MAJOR mistake (e.g., exposing private information or reporting confidential information), please let a supervisor know immediately so the school can take the proper steps to help minimize the impact it may have.

Netiquette

- Users should always use the Internet, network resources, and online sites in a courteous and respectful manner.
- Users should also recognize that among the valuable content online is unverified, incorrect or inappropriate content. Users should use trusted sources when conducting research via the Internet.

- Users should also remember not to post anything online that they wouldn't want parents, other staff members, or students to see . Once something is online, it's out there—and can sometimes be shared and spread in ways you never intended.

Personal Safety

- If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of your supervisor immediately.
- Recognize that communicating over the Internet brings anonymity and associated risks and should carefully safeguard your personal information and the personal information of others.

Cyberbullying

Cyberbullying will not be tolerated. Don't send emails or post comments with the intent of scaring, hurting, or intimidating someone else. Engaging in these behaviors will result in severe disciplinary action. In some cases, cyberbullying can be a crime. Remember that your activities are monitored and retained by others.

Examples of Acceptable & Unacceptable Use

I Will:

- Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
- Treat social media carefully. Alert a supervisor if there is any problem with their operation.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert a supervisor if I see threatening/bullying, inappropriate, or harmful content (images, messages, posts) online.
- Be cautious to protect the safety of myself and others.

I Will Not:

- Use social media in a way that could be personally or physically harmful to myself or others.
- Engage in cyberbullying, harassment, or disrespectful conduct toward others--staff or students.
- Try to find ways to circumvent the school's safety measures and filtering tools.
- Use language online that would be unacceptable in the classroom.

These are not intended to be exhaustive lists.Users should use their own good judgment when using social media.

Limitation of Liability

Highland Local Schools will not be responsible for damage or harm to persons, files, data or hardware.

Violations of these Social Media Guidelines

Violating these social media guidelines will result in disciplinary action or termination. This will be determined by Highland Local School Administration.

Acceptable Use Policy

Computer access is available to staff of the Highland Local School District. Personal electronic devices (Bring Your Own Technology) is permitted.

The Highland Local School District has taken precautions to restrict access to controversial materials in compliance to the Child Internet Protection Act (CIPA) of 2000. However, it is impossible to control all materials; an industrious user may discover controversial information. Highland Local Schools firmly believes that the valuable information and interaction available on the Internet far outweighs the possibility that users may procure material that is not consistent with the educational goals of the district.

The operation of the network relies on the proper conduct of the end users who must adhere to strict guidelines. The guidelines are provided so that users are aware of the responsibility of using computers and the Internet. This requires efficient, ethical and legal utilization of the network resources.

GUIDELINES

1. Privileges - The use of the Internet, school computers, and BYOT devices at school is a privilege, not a right. Inappropriate use will result in cancellation of these privileges and appropriate disciplinary measures.

2. Privacy - Network administrators may review communications to maintain system integrity and to insure that users are using the system responsibly. Users should not have the expectation of privacy on any BYOT device they use to access the Highland wireless system. The school reserves the right to search any privately owned BYOT device in accordance with applicable laws and policies.

3. Saving work - Users are required to use appropriate measures to save all of their work. Highland Local Schools is not responsible for any work lost due to user error, equipment or network failure. BYOT devices will only have internet access. No server access or printer access will be given to BYOT devices. Files must be saved via other means, such as flash drives, Remote Access, FTP, Google docs, etc.

4. Storage capacity - Users are expected to remain within allotted disk space and delete material that takes up excess storage space.

5. Email - The use of email is only permissible through school accounts assigned by the network administrators for appropriate school use.

6. Illegal copying - Users should never download or install any commercial software, shareware or freeware, unless they have permission from the Network Administrator. Users should not send or receive copyrighted materials in violation of US. Copyright law.

7. Inappropriate language, materials, images, music - Profane, abusive or impolite language should NOT be used to communicate, nor should materials be accessed which are not in accordance with the rules of school behavior. A good rule to follow is never view, send or access materials that you would not make public. Should users encounter such material by accident, they should report it immediately. Highland Local Schools determine what materials may violate these standards.

8. Other Usage - Computers are not to be used for commercial activity, personal business, political use, financial gain or for any illegal activity.

9. Reliability - Highland Local School District specifically denies any responsibility for the accuracy or quality of information obtained through the Internet.

Staff Computer and Internet Acceptable Use and Data Governance Agreement

GENERAL ACCESS

All staff members must have a current Acceptable Use and Data Governance Agreement on file with the Technology Department in order to access the Highland Local School District's network and any technology applications, including but not limited to: all computers, internet access, servers, student information system, and electronic grade book.

Name: _____

Building: _____

I understand and will abide by the provisions of the Highland Local Schools Computer and Internet Acceptable Use and the Data Governance Guidelines. I understand that any violations of the Acceptable Use or the Data Governance Guidelines will result in disciplinary actions. This could include revoking my user account and appropriate action by school authorities.

Printed Name:_____

Signature: _____ Date: ____/____/_____