



Delaware City Schools Technology Governance Guide

DCS Technology Department

Introduction

Delaware City Schools 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 technology 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 Technology 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.

Delaware City Schools is committed to not only maintaining strong privacy and security protections but also ensuring that the rules and principles of data protection are followed.

To listen to a podcast version of the DCS Technology Governance Guide,
[Click Here](#)

This audio overview was created using Notebook LM. NotebookLM, a Google AI tool, is a personalized AI research and note-taking assistant, that allows users to upload documents, generate summaries, and ask questions, utilizing the uploaded information.

Overview

It is Delaware City Schools' policy that all forms of data and information are protected from unauthorized disclosure, change, or destruction throughout its 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 Internet Acceptable Use Policy before accessing any district technical system. The Delaware City Schools' data policies and procedures will be made available to individuals responsible for their implementation and compliance.

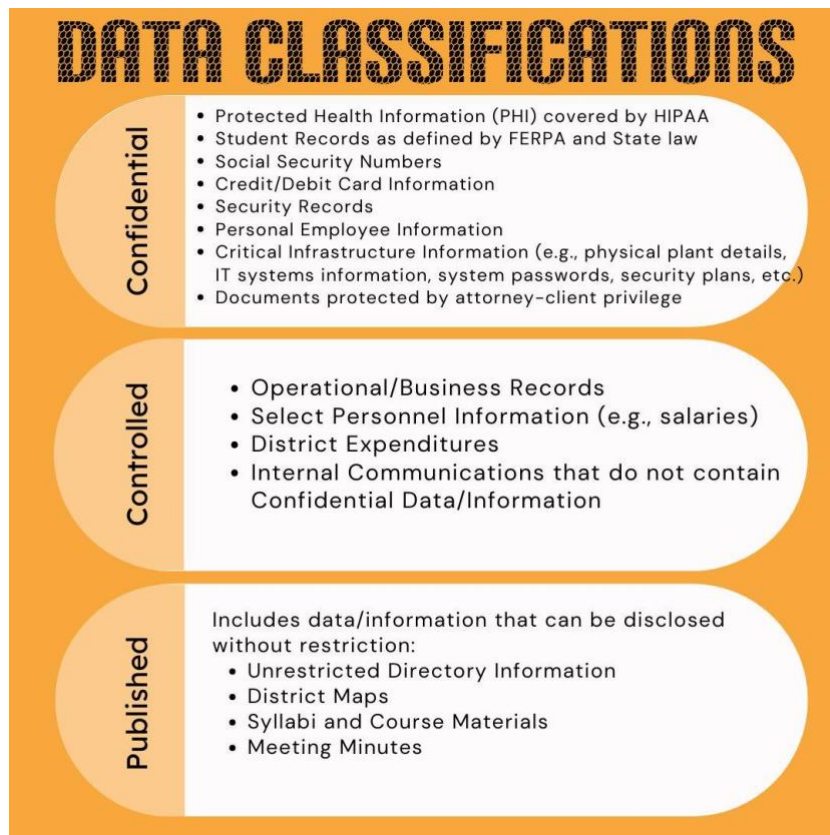
Scope and Regulations

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



Data and information include but are not limited to:

- A. Electronic data/information
- B. Data/information recorded on paper
- C. Data/information shared orally, visually, or by other means



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

“Published Data/Information”

Data/information made available to the public through posting to public websites, or distribution through e-mail, social media, print publications, or other media. This includes data/information that can be disclosed without restriction, such as unrestricted directory information, District maps, syllabi and course materials, and meeting minutes.

- No protection requirements for: collecting it, using it, granting access to it, sharing it, disclosing it, publicly posting/publishing it or electronically displaying it, exchanging it with third parties, services providers, cloud services, storing it on removable media, printing, mailing or faxing it or disposing of it (subject to District’s record retention policy, a litigation hold and administrative guidelines).

“Controlled Data/Information”

Data/information that is not generally created or made available for public consumption, but may be subject to release through a public records request or pursuant to another State or Federal law. This includes operational/business records, select personnel information (e.g., employees’ salaries), District expenditures, and internal communications that do not contain Confidential Data/Information.

- No protection requirements for: collecting or using it, storing it on removable media, electronically transmitting it, including emailing it or sending it via other electronic messaging services/apps, except reasonable methods shall be used to ensure Controlled Data/Information is only included in messages to authorized individuals with legitimate need-to-know access.

“Confidential Data/Information”

Data/information that is exempt or must be protected from unauthorized disclosure or public release based on State and/or Federal laws or regulations or applicable legal agreements. This includes “protected health information” covered by HIPAA, student records as defined by FERPA and State law, Social Security numbers, credit/debit card information, security records, personal employee information, critical infrastructure information (e.g., physical plant detail, IT systems information, system passwords, security plans, etc.), and documents protected by attorney-client privilege.

- Its collection and use are limited to authorized purposes as outlined in the District’s privacy policy. Departments or schools that collect and/or use Confidential Data/Information must use District-provided or approved servers, devices, systems, and/or processes to handle this type of data/information.
- Social Security numbers shall not be used to identify members of the District’s community if there are reasonable alternatives. SSNs shall not be used as a username or a password.
- Access shall be limited to authorized School District officials or agents with a legitimate academic or business interest and a need-to-know. All access shall be approved by an appropriate administrator.
- Before granting access to or exchanging Confidential Data/Information with third parties, service providers, cloud services, etc., contractual obligations
- Confidential Data/Information consists of:
 - "personal identifying information" as defined by State and Federal laws; This includes employer tax ID numbers, driver's license numbers, passport numbers, SSNs, State identification card numbers, credit/debit card numbers, banking account numbers, PIN codes, digital signatures, biometric data, fingerprints, passwords, and any other numbers or information that can be used to access a person's financial resources.
 - "protected health information" as defined by the HIPAA;
 - student "education records" as defined by the Family Educational Rights and Privacy Act (FERPA) and State law (R.C. 3319.321);
 - data/information that is deemed to be confidential in accordance with the Ohio Public Records Act;
 - "card holder data" as defined by the Payment Card Industry (PCI) Data Security Standard (DSS).

CIPA	PPRA	COPPA	HIPAA	FERPA	STATE
Children's Internet Protection Act	Protection of Pupils Rights Amendment	Children's' Online Privacy & Protection Act	Health Insurance Portability & Accountability Act	Family Educational Rights & Privacy Act (1974)	Legislation as well as Local Statutes and Regulations
Internet filters for K-12 schools and libraries to protect children from harmful online content as a condition for federal funding.	Requires parental consent for any surveys that contain political, sexual, mental state, relationships, religious information	Requires operators of websites or online services for children under 13 that they are collecting personal information	Usually HIPAA does not apply because information by definition is part of "education records" under FERPA and, therefore, is not subject to the HIPAA	Schools must have written permission to release any information but allows schools to disclose under certain conditions	40 states have passed 125 student privacy laws since 2013 laws

(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. Teachers must follow the DCS Digital Resource Approval Process prior to having students create digital accounts.

<https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>

(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>

(HIPAA) 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.

<https://www2.ed.gov/policy/gen/guid/fpco/ppra/parents.html>

Compliance

All Delaware City 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 District Technology 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 Delaware City Schools' board 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 Delaware City Schools' technological systems.
6. The intentional unauthorized altering, destruction, relocation, or disposal of Delaware City 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.
8. Using another user's account. This includes but is not limited to email, Chromebook, PC account and online software.

DCS Digital Approval Process

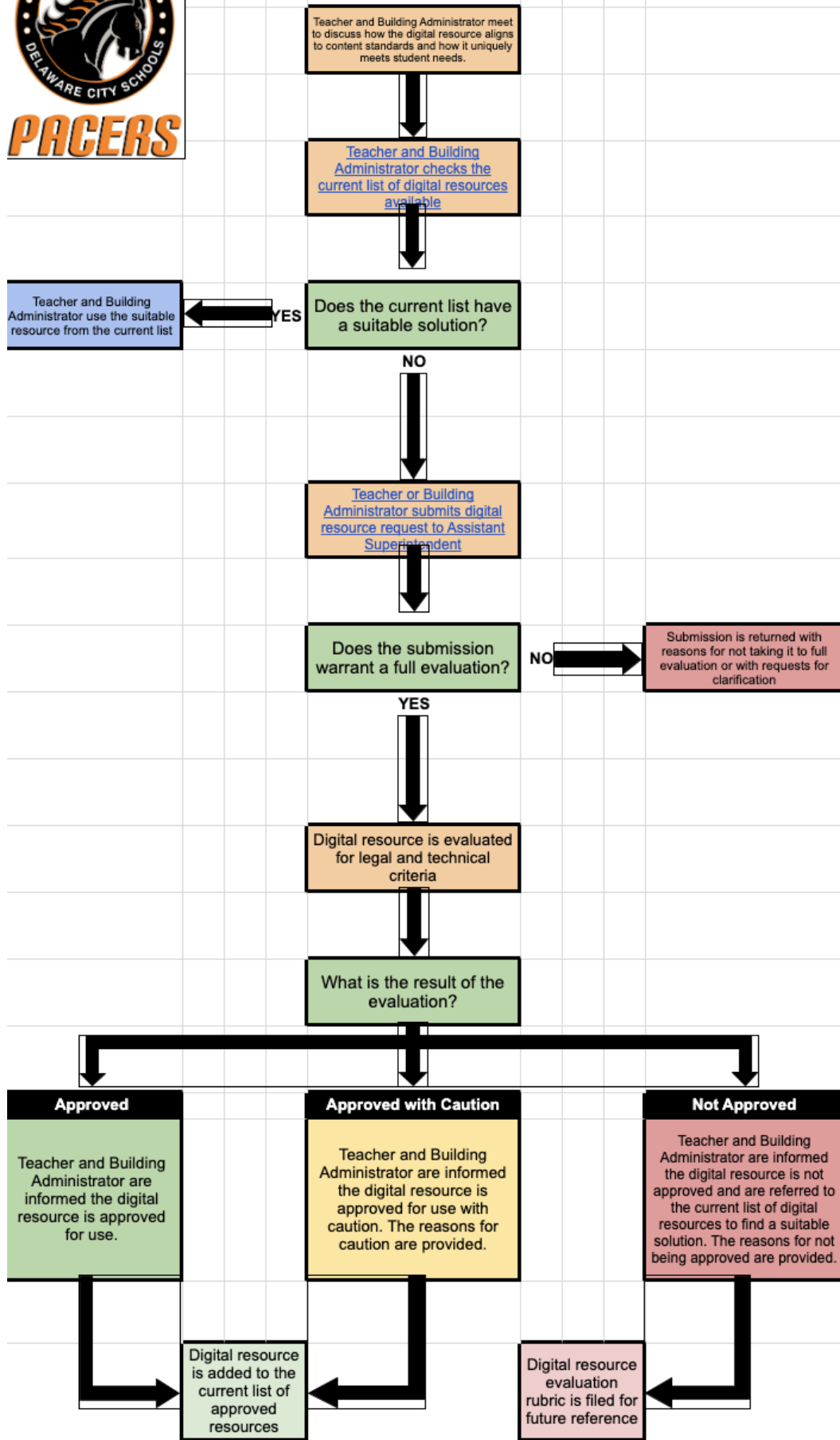
The district has a process in place for the vetting of new digital resources. Staff are required to complete the steps outlined in the Highland Technology Governance Committee flowchart below. Which can also be found on the district's website technology page.

The steps for getting a new digital resource approved are:

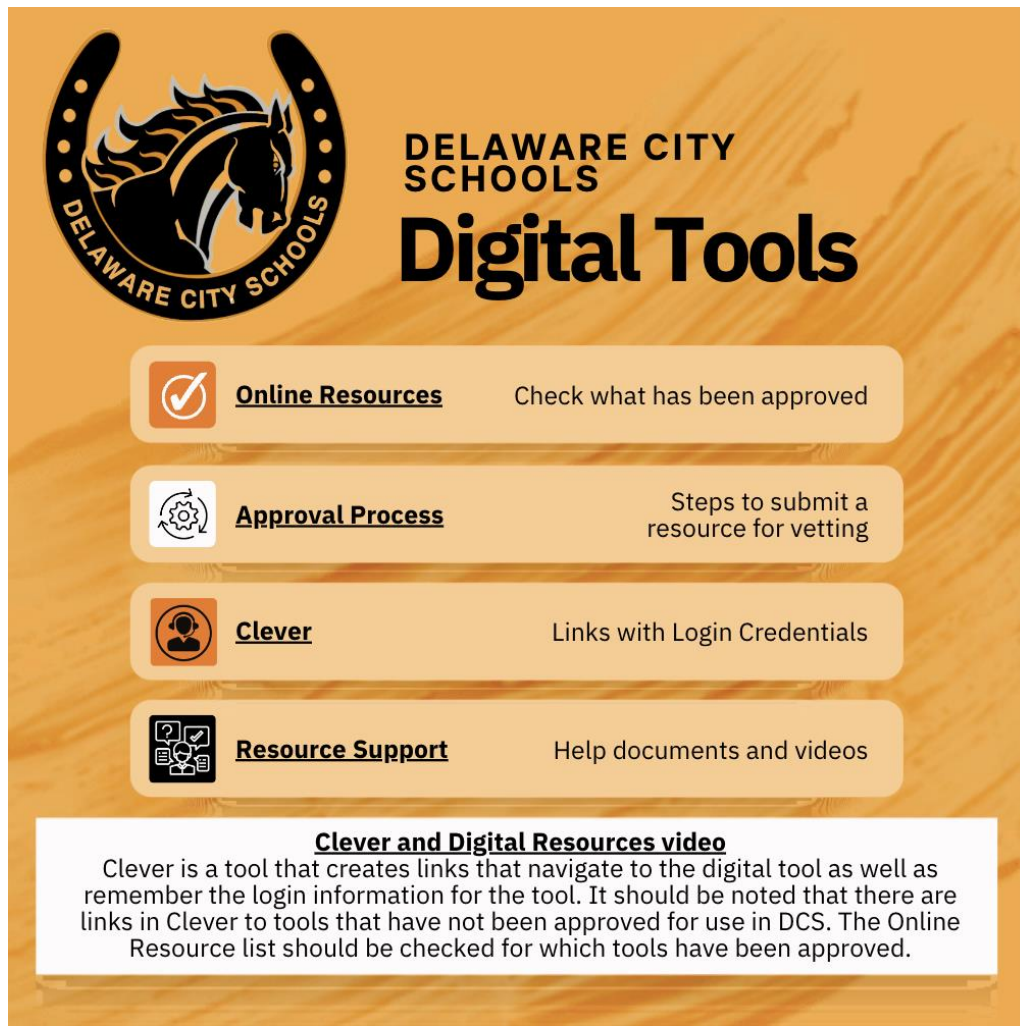
1. Teacher has an instructional conversation with school leadership regarding the alignment of the resource.
2. If school administrator agrees with the teacher on the need for the resource then they submit the request via the DCS website (digital resource request form)
3. Resource is discussed by the technology and curriculum teams for alignment to current district needs
4. If it's a suitable solution, a DPA is requested from the vendor and the teacher is notified.
5. DPA is either secured or not. If yes, the resource is approved. If no, the resource is not approved. Teacher is notified either way.
6. *Only approved district resources are to be used.*



DCS Digital Resource Approval Process



A list of evaluated software in use is maintained on the district website. 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.



The graphic features the Delaware City Schools logo on the left, which includes a horse head inside a horseshoe with the text "DELAWARE CITY SCHOOLS". To the right of the logo, the text "DELAWARE CITY SCHOOLS" is written in a smaller font, followed by "Digital Tools" in a large, bold font. Below this, there are four rounded rectangular buttons, each with an icon and text:

- Online Resources**: Check what has been approved (Icon: checkmark in a square)
- Approval Process**: Steps to submit a resource for vetting (Icon: gear with a checkmark)
- Clever**: Links with Login Credentials (Icon: person with a checkmark)
- Resource Support**: Help documents and videos (Icon: question mark, checkmark, and document)

At the bottom of the graphic is a white box with the following text:

Clever and Digital Resources video
Clever is a tool that creates links that navigate to the digital tool as well as remember the login information for the tool. It should be noted that there are links in Clever to tools that have not been approved for use in DCS. The Online Resource list should be checked for which tools have been approved.

[Delaware City Schools Digital Tools](#)

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 made on all employees with custom data access. Data Privacy Agreements (Contracts) with software providers are in place to ensure that data security standards are met.

Staff is responsible for securing the transmission of sensitive data. Secure data transfer protocol is in place for the regular transmission of student data to approved services (Gmail). Passwords should never be included in any communications. Transmission of student data to services such as 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 Delaware City 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 Delaware City 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 Delaware City Schools’ Records Retention Schedule and shredding guidelines should be made at the beginning of each school year. Student and employee records will be maintained per the district’s records retention schedule as outlined in board policy and administrative guideline 8310.

System Security

District employees will only have access to personal and confidential information if it is needed for their role. Each employee is placed into a specific security group in both the Student Information System (SIS) and Active Directory (AD). These systems have different groups, each with its own set of permissions to control who can access certain information.

A new employee notification is sent from the Human Resources Department to the Technology Department after board approval. This notification includes position, building assignment(s), start date and signed AUP, 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 the superintendent.

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). Delaware City 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 member of the district technology team. Long-term subs are given their own username/password and access to Delaware City Schools network.

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.). The existing password may not be reused when changing the password. Guest Wi-fi passwords will be changed quarterly.

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.

**KEEP IT SECRET,
KEEP IT SAFE!**

Your password protects your accounts and important data. Be sure to safeguard and protect it.

- Make it complex
- Don't share
- Change periodically

DCS Passwords require 12 characters including:
1 capitals, 1 lowercase, 1 number, 1 special character



Physical Security

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 an annual inventory verification of staff, classroom and student devices. Technology assets should be approved by the Technology Director/CTO 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. Please do not move technology assets without approval from the technology department. The technology department is responsible for inventorying technology equipment.

Use a district password-protected device to transport and store information. Do not put any PII on removable media such as USB drives or on personal devices and accounts. 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 or left overnight. Make sure your laptop is locked when unattended to secure against unauthorized use. When laptops are taken out of District, the laptop must be kept under control of the owner. It should be in hand, in sight or locked in a secure location at all times.

The Technology Director/CTO 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 are destroyed.



Virus, Malware, Phishing and Spam Protection

Delaware City Schools desktops, laptops, and file servers are protected using virus/malware software. All files and systems are scanned. An on-access scan is performed on all "read" files continuously. A PDQ server is used to keep all clients up-to-date with Microsoft patches. Servers, Hosts and Storage are patched and rebooted on an as needed basis.

To balance security on educational Internet resource and app use, for both production and guest networks, the Internet traffic from all devices that use these networks are routed through the district's content filter and firewall. This process sets the filtering level appropriately, based on the role of the user (e.g., student, staff, or guest). 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

Delaware City 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.

Critical Incident Response

Controls are in place so that the district can recover from damage to or breach of critical systems, data or information. Staff must immediately report security breaches (e.g. computer viruses, hacking attempts) to their supervisor and the technology department.

The district will maintain near-live, offsite and long-term 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 efficiently restore any loss of data.

Delaware City Schools will also maintain an Incident Response Plan (AG 8305.b) 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 analyzing 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 Incident Response Team.