

## **Dodge County Schools Logical Access Process**

The following procedure for requesting, granting, and modifying access to data contained within Dodge County Schools is designed to ensure that requests for access receive appropriate approvals and are fully auditable. This procedure includes the steps to request, authorize, modify, review and revoke access to Dodge County Schools' data.

The Building Level Administrator or a Department Head has to email the Director of Technology identifying new hires or request for modifications to a user's rights in their building or departments. The Director of Technology and the Technology Department will have the final decision of creating new users or modifying users. In the case of an employee leaving the system the Principal of that building or Department Head must notify the Technology Department by email.

The Technology Department will review all users' access in the district annually. They will ensure all user have the appropriate rights granted for their station.

# Incident Response Plan

- 1) The person who discovers the incident will immediately contact the Dodge County Schools Technology Department. Depending on the severity of the incident the following Incident Response Team will be notified.
  - a) Director of Technology (Rick Rogers) 478-231-4939 24/7
  - b) Educational Technology Specialist (Clay Hall) 478-231-9119
  - c) Educational Technology Specialist (Jennifer Lee) 478-231-8037
  - d) Superintendent (Dr. Susan Long) 478-278-7878
  - e) Federal Programs (Dr. Denise Brown) 478-231-9368
  - f) Chief Financial Officer (Georgette Evans) 478-231-5104
  - g) School Nutrition (Dena Barrows) 229-332-0032
  - h) Director of Safety (Davey Sheffield) 478-231-1254

Also each building administrator shall be notified and our network engineer (Matt Boyette 478-278-6453) will need to be notified.

- 2) If the person discovering the incident is not a member of the IT department or affected department, they will call the Director of Technology at 478-231-4939.
- 3) The Director of Technology will log the following information:
  - a) The name of the caller.
  - b) Time of the call.
  - c) Contact information about the caller.
  - d) The nature of the incident.
  - e) What equipment or persons were involved?
  - f) Location of equipment or persons involved.
  - g) How the incident was detected.
  - h) When the event was first noticed that supported the idea that the incident occurred.

Once this information is gathered it will be decimated to Jennifer Lee (Educational Technology Specialist). Mrs. Lee will maintain all documentation after the initial log documented by the Technology Director.

- 4) The Director of Technology or the Technology Department staff member who receives the call (or discovered the incident) will refer to their contact list for both management personnel to be contacted and incident response team members to be contacted. The staff member will call those designated on the list. Mrs. Lee will document the following

- a) Is the equipment affected business critical?
  - b) What is the severity of the potential impact?
  - c) Name of system being targeted, along with operating system, IP address, and location.
  - d) IP address and any information about the origin of the attack.
- 5) Contacted members of the response team will meet or discuss the situation over the telephone and determine a response strategy.
- a) Is the incident real or perceived?
  - b) Is the incident still in progress?
  - c) What data or property is threatened and how critical is it?
  - d) What is the impact on the business should the attack succeed? Minimal, serious, or critical?
  - e) What system or systems are targeted, where are they located physically and on the network?
  - f) Is the incident inside the trusted network?
  - g) Is the response urgent?
  - h) Can the incident be quickly contained?
  - i) What type of incident is this? Example: virus, worm, intrusion, abuse, damage or Ransomware.
  - j) If the incident is Ransomware, do we pay the ransom?
- 6) An incident ticket will be created. The incident will be categorized into the highest applicable level of one of the following categories:
- a) Category one - A threat to public safety or life.
  - b) Category two - A threat to sensitive data
  - c) Category three - A threat to computer systems
  - d) Category four - A disruption of services
- 7) Once the incident is access, GSBA will be notified. GSBA will instruct Dodge County Incident Response Team what entities to contact. GSBA will also contact their legal department to support Dodge County Schools. The Technology Department will also contact Georgia Department of Education and GEMA.  
GSBA Claims-Cyber 888-245-4722 ext. 26  
GEMA 800-879-4362  
Chris Shealy (DOE) 404-657-3533
- 8) Team members will use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused. Only

- authorized personnel should be performing interviews or examining evidence, and the authorized personnel may vary by situation.
- 9) Team members will recommend changes to prevent the occurrence from happening again or infecting other systems.
  - 10) Upon the Superintendent's approval, the changes will be implemented.
  - 11) Team members will restore the affected system(s) to the uninfected state using the following steps:
    - a) Re-install the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.
    - b) Make users change passwords if passwords may have been sniffed.
    - c) Be sure the system has been hardened by turning off or uninstalling unused services.
    - d) Be sure the system is fully patched.
    - e) Be sure real time virus protection and intrusion detection is running.
    - f) Be sure the system is logging the correct events and to the proper level.
  - 12) Documentation—the following shall be documented:
    - a) How the incident was discovered.
    - b) The category of the incident.
    - c) How the incident occurred, whether through email, firewall, etc.
    - d) Where the attack came from, such as IP addresses and other related information about the attacker.
    - e) What the response plan was.
    - f) What was done in response?
    - g) Whether the response was effective.
  - 13) Evidence Preservation—make copies of logs, email, and other communication. Keep lists of witnesses. Keep evidence as long as necessary to complete prosecution and beyond in case of an appeal.
  - 14) Assess damage and cost—assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.
  - 15) Review response and update policies—plan and take preventative steps so the intrusion can't happen again.
    - a) Consider whether an additional policy could have prevented the intrusion.
    - b) Consider whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future.
    - c) Was the incident response appropriate? How could it be improved?

- d) Was every appropriate party informed in a timely manner?
- e) Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved?
- f) Have changes been made to prevent a re-infection? Have all systems been patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?
- g) Have changes been made to prevent a new and similar infection?
- h) Should any security policies be updated?
- i) What lessons have been learned from this experience?

# **Dodge County Schools Remote Access Procedure**

Dodge County Schools recognizes that some faculty and staff need to access data from Dodge County Schools when they are not physically on the campuses of Dodge County Schools. The purpose of this procedure is to state the requirements for remote access to data of Dodge County Schools.

1. While connected to Dodge County Schools' computing resources, remote access users are required to follow Dodge County Schools policies at all times, including the Acceptable Use Policy.
2. All remote devices set forth in the scope of this document must have appropriate security protections enabled. These protections include but are not limited to the use of anti-virus software with the latest definitions installed, all appropriate operating system security patches applied and a personal firewall installed.
3. Any remote access user who is utilizing a VPN Gateway should remain connected for only as long as they are conducting business-related work for Dodge County Schools and are encouraged to disconnect as soon as their work is completed.
4. Remote access users are not permitted to download or otherwise store Dodge County Schools' data which is considered confidential or contains Personal Identifiable Information on their personal remote computing device. This includes the transfer of such data to a personal cloud service such as Google Drive or Dropbox.
5. If any device used for remote access is lost or stolen, or otherwise removed from a user's control, the authorized user will be responsible and immediately contact the Dodge County Schools Technology Department.
6. Remote access users agree to immediately report to the Technology Department any incident or suspected incident of unauthorized access and/or disclosure of any company resources or information.
7. The Director of Technology will have to approve all remote users with access to the District's resources.

# **Dodge County Schools IT Risk Assessment**

## **Procedure**

The purpose of an IT Risk Assessment is to ensure all vulnerabilities and shortfalls of the Dodge County Schools' network are addressed and managed properly. The Technology Department will provide professional development to all staff of Dodge County Schools to inform them about IT Security Risk. Dodge County Schools contracts with a network engineer. The network engineer will perform a risk assessments quarterly. The network engineer will give a verbal report of his findings to the Director of Technology. The findings will be addressed by the network engineer and the Director of Technology.

# **Dodge County Schools IT Hiring and Retention Plan**

The Director of Technology, the Superintendent, and interview team will interview potential candidates for Technology Specialist positions. In the case of the Director of Technology position be vacated. The Superintendent and his or her designees will interview potential applications for the position of Technology Director.

The retention plan for retaining staff is the Director of Technology will have daily meetings with the Technology Department to keep them abreast of any problems or concerns. The Director of Technology will also ensure that the Technology Staff will have ample opportunities for professional growth and development.

# Dodge County School District

## IT Security Incident Response Plan

---

3/12/2020

**Author: Rick Rogers**

**Approved by Superintendent, Dr. Susan Long**

**Table of Contents**

Purpose ..... 1

Incident Identification, Containment, and Classification (stage one)..... 1

    Risk Categories ..... 3

    Classification Levels..... 3

Investigation (stage two) ..... 4

Notification/Alerting and Responding (stage three)..... 4

    Escalation ..... 4

Reporting and Documentation (stage four)..... 4

IT Security Incident Response Communications Plan ..... 6

    Priority 1 (Low)..... 6

    Priority 2 (Medium)..... 6

    Priority 3 (High) ..... 6

IT Security Incident Response Guidelines ..... 7

DCS IT Security Incident Response Form ..... 9

# *Dodge County School District IT Security Incident Response Plan*

---

## **Purpose**

The purpose of this plan is to protect the confidentiality, integrity and availability of Dodge County School District (“DCS”) data. The proper handling of information technology security incidents (hereinafter referred to as “security incidents”), both electronic and physical, is critical in protecting DCS. These procedures are intended to coexist with all other legally binding documents that guide the conduct of DCS employees

*The IT Security Incident Response Plan is organized into four stages.*

## **Incident Identification, Containment, and Classification (stage one)**

A security incident is a real or perceived threat which exploits or attempts to exploit vulnerability. All DCS employees are responsible for identifying and reporting possible security incidents. While some security incidents appear to be easily identified and understood, others require review and analysis to make a determination about the nature and scope of the problem. Many DCS employees will not be able to confirm a security incident, thus any abnormal events should be reported promptly. Examples of events which should be reported are:

- ❑ Password alterations not initiated by the user;
- ❑ Internet browser pop-ups that cannot be closed;
- ❑ Workstation infection from a virus, worm, spyware or other malicious software;
- ❑ Missing physical files that contain data classification Level 1, Level 2, or Level 3 information;
- ❑ Loss or theft of DCS keys which allow facilities access;
- ❑ Loss or theft of DCS computer hardware; and
- ❑ Loss or theft of any mobile computing device.

All DCS employees must report these and other suspicious events immediately to a member of the Data Center IT Staff (hereinafter referred to as “Data Center”) at 478-374-3783 and or to the Director of Technology during normal business hours. All after-hours security incidents must be reported as soon as possible to the employee’s supervisor. Loss or theft of DCS real or personal property must be reported to the Facilities Director.

Here are some general guidelines that should be followed during a possible security incident:

- ☐ If your password has been compromised, report this matter immediately to the Technology Department ;
- ☐ If you have reported a security incident, do not continue working on the computer, or in the case of a physical security incident do not continue working in that area;
- ☐ Do not close computer applications, or alter the work area (close or move physical documents, etc.) as this may destroy useful information;
- Do not resume using a workstation or a work area until it is declared 'safe' by the Data Technology Staff; and
- Only discuss the security incident with the Technology Staff. Only the Technology and the Administrators are allowed to communicate information about a security incident.

When reporting a potential security incident attention to detail is very important. Keep track of the time and what activities were being performed (in detail) when the potential security incident is discovered. By recording these facts, the Technology Staff will have better information by which to respond to the security incident. **All incidents should also be recorded in the DCS technology ticketing system regardless of severity.** The important details to include in reporting a security incident are:

- ☐ Name, location, telephone number and workstation name if applicable;
- ☐ A detailed description of the potential security incident or abnormal event(s);
- ☐ The date(s) and time(s) of when the potential security incident or abnormal event occurred; and
- ☐ Any other additional information which can be obtained without affecting or making worse the security incident or which could alert a potential or confirmed perpetrator that someone is aware of their actions or presence.

**The Technology Staff will begin the documentation process.**

Security incidents fall within one of three risk categories. In addition, each of these categories will be associated with a security incident classification level. **IT Security Incident Communications** will be based upon the priority assigned to the security incident. A priority will be assigned to each security incident upon examination and review of the event. Loss, theft or unauthorized disclosure of personally identifiable information will follow the communication requirements as described by law.

Only communications authorized by the Director of Technology and Superintendent's Office may communicate information about a security incident. Communicating information haphazardly about a security incident could further increase the risk to DCS.

### Risk Categories

Risk	Description
Low	A security incident localized to no more than two individuals and which includes data classification Level 1 information. Security incidents at this level include loss of physical or electronic data which is of limited risk to DCS.
Medium	A security incident which disrupts normal work (workstation, local area network, work area). Security incidents at this level may include loss, theft, or unauthorized disclosure of data classification Level 1 or Level 2 information (but which does not include personally identifiable information). Security incidents at this level are of moderate risk to DCS.
High	A security incident which affects a large number of users or which effects data classification Level 2 or Level 3 information (including any personally identifiable information). Security incidents at this level are of extreme risk to DCS.

### Classification Levels

Level		Examples
Low	Low level security incidents have minimal impact to information systems or data.	<ul style="list-style-type: none"> <li>Loss, theft, or unauthorized disclosure of data that has minimal impact or risk to DCS or its stakeholders;</li> <li>Vulnerabilities that can be completely mitigated by changes in configurations, policy, procedure, or through technology; and</li> <li>Loss, theft, or unauthorized disclosure of a DCS portable or removable storage device that contains data classified as Level 1 and which is not encrypted.</li> </ul>
Medium	Medium security incidents affect the availability of services or data.	<ul style="list-style-type: none"> <li>Loss, theft, or unauthorized disclosure of electronically stored data classified as Level 2 or Level 3 electronically stored data which is not encrypted and which does not include personally identifiable information;</li> <li>Loss, theft, or unauthorized disclosure of physical information which contains data classified as Level 2 or Level 3 and which does not include personally identifiable information; and</li> <li>Any security incident which allows an intruder access at a level less than privileged, which could lead to further opportunity to obtain greater access whether electronic or physical.</li> </ul>
High	Severe security incidents affect critical information systems or data.	<ul style="list-style-type: none"> <li>Virus, worm, or other malicious code propagation without user action;</li> <li>A security incident which allows an intruder to gain privileged access (admin/root) to a system;</li> <li>A security incident which allows an intruder to gain unauthorized physical access to a secured facility;</li> <li>The physical or electronic compromise of confidentiality, integrity, availability of data or the integrity or availability of processing resources;</li> <li>Loss, theft, or unauthorized access and/or dissemination of personally identifiable information whether physical or electronic;</li> <li>Loss, theft, or unauthorized disclosure of physical information (manual records) classified as Level 2 or Level 3;</li> <li>Loss, theft, or unauthorized disclosure of electronic data classified as Level 2 or Level 3 which is not encrypted.</li> </ul>

## Investigation (stage two)

In the investigation stage, the Technology Staff will gather all known information regarding the security incident and will correlate any information regarding the current incident to any other incidents and abnormal events to determine the urgency and the scope of the issue. Criteria that determine the severity and urgency are:

- ☐ Business Criticality
- ☐ System Availability
- ☐ Data Availability
- ☐ Level of current functionality
- ☐ Effect on employee productivity
- ☐ Lack of alternative workarounds
- ☐ Data classification level of information
- ☐ Loss, theft, unauthorized disclosure of personally identifiable information

If it is determined that no security incident has occurred, the suspected incident will be labeled as an event and closed by the Technology Staff. If the risk is determined to be low, it will be documented in the DCS technology ticketing system only and closed. No form will be completed.

## Notification/Alerting and Responding (stage three)

In the notification and response stage the Data Center will determine the scope of the security incident, the immediate impact, and initiate the required response. Escalation and communication alerts are the responsibility of the Director of Technology. Should the security incident meet any of the following criteria, the escalation process should be immediately followed:

- ☐ Security incident has an immediate enterprise wide impact;
- ☐ Security incident meets legal requirements that require disclosure; or
- ☐ Security incident has caused a business critical service interruption.

Attachment A details the IT Security Incident Response Communications Plan and priorities that the Technology Staff will follow.

## Escalation

In the event that the security incident has immediate impact on DCS as a whole, the Technology Staff investigating the security incident will promptly notify the Director of Technology. Certain security incidents may require reporting or alerting of outside third parties or vendors.

## Reporting and Documentation (stage four)

All Level 2 and 3 security incidents will be documented through the use of the IT Security Incident Response Form. All employees involved in a security incident are required to provide feedback and documentation on their involvement in the process. At a minimum, the report will contain the following information collected during each stage of a security incident investigation:

- ☐ Name, location, telephone number and workstation name if applicable;
- ☐ A detailed description of the potential security incident or abnormal event(s);
- ☐ The date(s) and time(s) of when the potential security incident or abnormal event occurred; and

- ☐ Any other additional information which can be obtained without affecting or making worse the security
- ☐ incident or which could alert a potential or confirmed perpetrator that someone is aware of their actions or presence;
- ☐ Technology Staff member who investigated the security incident;
- ☐ Cause of the security incident (if apparent);
- ☐ Employee(s) involved;
- ☐ Action(s) taken;
- ☐ Resolution;
- ☐ Date completed;
- ☐ Business impact;
- ☐ Damage caused;
- ☐ Lessons learned;

Planned future mitigation (if possible).

Attachment B provides guidance in developing a detailed security incident response report.

## IT Security Incident Response Communications Plan

**IT Security Incident Communications** will be based upon the priority assigned to the security incident. A priority will be assigned to each security incident upon examination and review of the event. Loss, theft or unauthorized disclosure of personally identifiable information will follow the communication requirements as described by law.

Only communications authorized by the Coordinator of Director of Technology and Superintendent's Office may communicate information about a security incident. Communicating information haphazardly about a security incident could further increase the risk to DCS.

**Priority 1 (Low)** security incidents require the teacher or staff member to enter a ticket into the DCS technology ticketing system, if not already entered and notify designated persons of the affected areas as required. If ticket is already created, the person will be notified by the system upon commencement of work. In the event that the DCS technology ticketing system is unavailable, the information will be dispersed by telephone or email. The communication will state:

- ☐ What non-critical device/system is affected;
- ☐ That the incident is being worked on; and
- ☐ Estimated time to resolution.

**Priority 2 (Medium)** security incidents require the Director of Technology to create an e-mail which will be sent to the Administrators and to other designated persons as required. In the event that DCS's e-mail system is unavailable, the information will be dispersed by telephone. The communication will state:

- ☐ What the security incident is;
- ☐ What workstation, device, laptop, etc., has been affected;
- ☐ That the incident is being worked on; and
- ☐ Estimated time to resolution.

**Priority 3 (High)** security incidents require the Director of Technology to create an e-mail for dispersion that will be delivered to all persons affected. In addition, the Director of Technology will notify the main point of contact for all facilities affected by telephone. The communication will state:

- ☐ What the security incident is;
- ☐ What systems or availability of systems the incident has affected;
- ☐ That the incident is being worked on;
- ☐ Estimated time to resolution;
- ☐ Updates will be forthcoming; and
- ☐ State any prescribed course of action the customers must take until the incident is resolved.

## IT Security Incident Response Guidelines

**IT Security Incident Response Reports** are required on all security incidents that the Technology Department responds to. The following information is provided as a guideline for developing detailed security incident response reports. At the conclusion of each report, there must be a recommended course of action that specifies what should be done to prevent the future reoccurrence of the security incident.

### Preparation

- Were detection capabilities in place that discovered this incident?
- Were security controls in place to prevent the security incident?
- What conditions allowed the security incident to happen?
- What could have prevented this security incident?
- Was this security incident reported promptly?

### Detection

- How soon after this security incident occurred was it detected?
- What could have been done to detect this earlier?
- Was the IT Security Incident Response Policy followed?
- Did the Data Center respond in a prompt manner?
- Were the required parties informed of the security incident?

### Containment

- How quickly was the security incident contained?
- What was done to contain the security incident?
- If services were disrupted to DCS to contain this security incident, was the Director of Technology notified?
- If services were disrupted to DCS to contain this event, was DCS Technology Staff notified?
- Could changes be made to the environment that would have made containing the security incident easier or faster?
- Were all containment actions documented?
- Was criminal activity involved?
- Was appropriate action taken or sought?
- Criminal intent?
- Was notification completed as required by law or statute?

### Corrective Action

- Was the security incident corrected?
- Was data recovered if involved, and was any data permanently lost or compromised?
- How were corrective actions prioritized if the security incident covered multiple devices, systems, or locations?

- ☐ Were the necessary tools readily available to support the corrective actions taken?
- ☐ Did the staff have the necessary training to determine and implement the necessary corrective actions to remedy the security incident?

### **Incident Review**

- ☐ What could be done to prevent this security incident from reoccurring?
- ☐ What security controls could be put in place to protect or detect against security incidents of this nature?
- ☐ What training or education could be implemented to solve or prevent security incidents of this type?
- ☐ What was learned from this security incident?

## DCS IT Security Incident Response Form

<b>1. Contact Information (person reporting the Incident)</b>		
Name	Cost Center:	Phone Number:
<b>2. Security Incident Details</b>		
Date and Time Reported:	Date and Time Discovered:	Reported To:
Incident Category:	Incident Classification Level:	Source (IP if known):
<input type="checkbox"/> External	<input type="checkbox"/> Level 3 – Severe	
<input type="checkbox"/> Internal	<input type="checkbox"/> Level 2 – Medium	
<input type="checkbox"/> Physical	<input type="checkbox"/> Level 1 – Low	
Incident Description:		
Resources Affected:		
<b>3. Actions Taken (Including Ticket Information):</b>		
<b>4. Incident Assessment:</b>		
Technical Impact of the Incident:		
Information/Data Lost:		
Business Impact of the Incident:		
Severity of Incident:	Loss of business hours:	Loss of IT hours:
<b>5. Incident Categorization (Check which apply)</b>		
<input type="checkbox"/> Virus or Worm	<input type="checkbox"/> Unauthorized Access	<input type="checkbox"/> DoS Attack
<input type="checkbox"/> Compromised User Access	<input type="checkbox"/> Policy Violation (e-mail)	<input type="checkbox"/> Policy Violation (Internet)
<input type="checkbox"/> Loss of Laptop	<input type="checkbox"/> Loss of Portable Device	<input type="checkbox"/> Loss of Data
<input type="checkbox"/> Other (Specify):	<input type="checkbox"/> Loss of PII	<input type="checkbox"/> Physical Intrusion
	<input type="checkbox"/> PII involved?	<input type="checkbox"/> Student Data Involved?
6. Shared with Coordinator? <input type="checkbox"/> Yes <input type="checkbox"/> No		
7. Risk Management Notified?		
8. Superintendent Notified?		

# DODGE COUNY SCHOOLS ANTI-VIRUS PROCEDURE

## **Purpose**

This policy is designed to prevent viruses, malware, or malicious code from infecting Dodge County Schools computing devices and network. By preventing infection, data, files, and resources will also be protected. This procedure shall be reviewed for content and compliance by the Technology Director or designee on an annual basis.

## **Scope**

This procedure applies to all computers that are connected to the DCSS network via a standard network connection, wireless connection, or virtual private network connection. This includes both Dodge County Schools-owned computers and personally-owned computers attached to DCSS's network.

## **Procedure**

All computers attached to DCSS'S network must have anti-virus software installed with current virus definitions. This includes, but is not limited to, desktop computers, and laptop computers. Any activities with the intention to create and/or distribute malicious programs onto the DCSS network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited, in accordance with Dodge County Schools Technology Acceptable Use Policy. No student, faculty, staff, or guest should attempt to destroy or remove a virus, or any evidence of that virus, without direction from DCSS Technology Department. Any virus-infected computer will be removed from the network and remain off the DCSS network until it is verified as virus-free by DCSS Technology Department.

### *Department and Individual Responsibilities*

The following activities are the responsibility of DCSS departments and employees:

1. Departments must ensure that all departmentally-managed computers have virus protection that is in keeping with the standards set out in this procedure.
2. All employees and students are responsible for taking reasonable

measures to protect against virus infection.

3. Employees nor Students must not attempt to either alter or disable anti-virus software installed on any computer attached to the DCSS network without the express consent of the DCSS Technology department.

## **Enforcement**

Any student/employee/faculty member who is found to have violated this procedure may be subject to disciplinary action.

# **Dodge County Schools Change in Management**

## **Procedure**

In the event the Director of Technology takes employment elsewhere or is physically or mentally unable to complete his or her assigned duties, the Technology Specialists will split the assigned roles of the Director of Technology. This will be the case until a suitable replacement can be found. Additionally, if the Director of Technology takes other employment or is physically or mentally unable to do his or her duties, all administrator rights must be taken from that individual immediately.

# Dodge County Schools Backup Procedure

Dodge County Schools Technology Department will be responsible for maintaining backups of all file servers and critical data servers (PC Genesis and the Food Service Server). Information on these servers will be backed up every evening when work day has completed. Dodge County Schools will have 6 months of retention of all data on the servers. It will have onsite retention and off site retention.

The Director of Technology will receive emails daily to make sure the accuracy of these backups. If a failure occurs in these backups. The Director of Technology will inform the company that provides our backup solution. This company will be responsible for remediating this issue.

Dodge County Schools Technology Director will also be responsible for testing these backups' on an annual bases. The IT Director will restore a backup copy all critical data servers.



# *Dodge County Schools*

**Dr. Susan W. Long, Superintendent**

720 College Street

Eastman, Georgia 31023

Telephone (478)374-3783

## **ACCEPTABLE USE COMPUTER POLICY**

The Dodge County Schools Computer Network is established for the educational and professional use of Dodge County Schools' students, faculty, and staff ("Users"). This Technology and Acceptable Use Policy (the "Policy") is intended to govern Users with respect to Dodge County Schools Network and the Internet. Users are expected to conduct themselves on the Dodge County Schools Network in the same fashion as they do elsewhere in the community. Users who violate this Policy will have their Dodge County Schools Network privileges revoked and may be subject to further disciplinary action, including suspension or dismissal. Dodge County Schools may also report offenders to applicable law enforcement agencies.

The Dodge County Schools Network provides access to the global Internet. Dodge County Schools have taken available precautions to restrict access to controversial materials on the Internet. However, on a global network, it is impossible to control all materials. Dodge County Schools believe that the valuable information and interaction available on the Internet far outweighs the possibility that Users may find material that is not consistent with our educational goals.

The smooth operation of the Dodge County Schools Network relies upon the proper conduct of all Users. The signature on the Handbook Acknowledgement form is legally binding and indicates the parties who have signed have read the terms and conditions of this Policy carefully and understand their significance.

### **Dodge County Schools Network - Terms and Conditions (Acceptable Use and Illegal Actions)**

Scope and Authority – The Dodge County Schools Network includes all hardware, software, and network services used by the Dodge community. Parents give the school permission to use applications that are educationally beneficial to our students.

### **Privileges**

The use of the Dodge County Schools Network is a privilege, not a right. The use of an account must be consistent with the educational objectives of Dodge County Schools. The Technology Office and/or School Administration will deem what is inappropriate use and will refer any such conduct to Dodge County Schools Administration. Dodge County Schools, in its sole discretion, reserves the right to determine what conduct constitutes a violation of this Policy, and the discipline for any such violation. Transmission of any material in violation of any U.S. or state regulation is prohibited. This includes, but is not limited to, material protected by copyright, threatening or

obscene material, or material protected by trade practice. Use of the Dodge County Schools Network for commercial activities, product advertisement, or political lobbying is prohibited. Use of the Dodge County Schools Network and the Internet must be consistent with this Policy and all policies and practices of Dodge County Schools, and violations of this Policy and such other policies and practices may result in the suspension or loss of an account, loss of Internet access, or in other forms of disciplinary action.

### **No Expectation of Privacy**

Dodge County Schools routinely monitor usage of the Dodge County Schools Network and may review any communications on its systems. Dodge County Schools is able to override all passwords. Users do not have a privacy right in the contents of their computer system, including messages sent, received, or stored on the email systems or in their use of the Internet. Passwords to these systems exist for the benefit of Dodge County Schools. Users should have no expectation that the ability to choose a password for a system in any way limits the ability or right of Dodge County Schools to monitor all activity.

### **Security**

Security on any computer system is a high priority, especially when the system involves many Users. No User may have access to another's files on the Dodge County Schools Network. The following guidelines will help maintain Dodge County Schools Network security:  
If you feel you have identified a security problem on the Internet, you must notify the Director of Technology.

Do not allow anyone else to use your account and do not use another individual's account. Inappropriate attempts to access a server as an administrator will result in immediate cancellation of User privileges and/ or discipline.

Any User identified as a security risk or having a history of problems with other computer systems may be denied access to the Dodge County Schools Network.

### **Inappropriate Access**

Not all of the information freely available on the Internet is reliable or helpful. Students and employees must evaluate the source of the information, as well as the information itself, to determine its appropriateness and usefulness.

In addition to providing information, the Internet is capable of providing the means to communicate directly with others via "instant or private messaging" programs, video conferencing programs, and other means. Also, there are many places and software technologies that will allow for the free exchange of files between computers over the Internet, such as email. Not all of these methodologies are appropriate for an educational environment as outlined in this document.

Downloading or loading of software on Dodge County Schools' computers is prohibited. There is an enormous quantity and variety of free software available on the Internet. However, widespread downloading of such software on the School's computers has a cumulative negative effect, and can result in the substantial degradation of performance, additional maintenance time, and increased threat of virus infestation. All software purchases must be approved by the technology staff.

Students may not use school computers to access any Internet site or sites that contain information that is inappropriate for educational purposes or sites that teachers, staff or administration deem inappropriate for the instructional program. Examples of inappropriate information and/or content include, but is not limited to, the following:

Students may not access, upload, download, transmit, display or distribute:

- a.) offensive material – content that is in poor taste or could be considered obscene; abusive or sexually explicit language, racist, illegal, harassing or inflammatory.
- b.) distribute dangerous material – content that provides direction in the construction of explosives or similar devices or instruction or practices that could injure the students themselves or others.
- c.) inappropriate contacts – materials that can lead to contact with strangers who could potentially threaten the student's health or safety.

If a student is uncertain as to whether or not a site's material might be considered inappropriate, the student should consult his or her teacher or a member of the administrative staff for clarification.

## **Privacy**

School staff and administrators have access to student email for monitoring purposes. Students should have no expectation of privacy on the Google Apps for Education system.

Limited personal use - Students may use Google Apps for Education tools for personal projects but may not use them for:

- Unlawful activities.
- Inappropriate sexual or other offensive content.
- Threatening another person.
- Misrepresentation of Dodge County Schools, staff or students.

## **Safety**

Students will tell their teacher or other school employee about any message they receive that is inappropriate or makes them feel uncomfortable.

Students are responsible for the use of their individual accounts and should take all reasonable precautions to prevent others from being able to use their accounts.

Under no conditions should a user provide his or her password to another person.

## **Access Restriction - Due Process**

Due to the rapidly changing technology environment, Dodge County Schools reserve the right to determine if an action not listed in this document is inappropriate, and the student may be subject to discipline.

## **Hardware**

Student Chromebooks/Devices are managed in order to allow for student use of systems only for educational purposes. Under no circumstances is a student to attempt to modify the existing hardware configuration. Modification can be considered either opening the case or changing hardware or software settings. Students are responsible for any damage on their computers.

Dodge County Schools Information Technology offers a Guest Network for connection purposes.

## **Contact**

Each student and employee is responsible for all activity that occurs under his/her user account. Students and employees may not place information on the Internet that is inappropriate or unacceptable.

Students may not give out any personal information (e.g., address, phone number, user name, passwords, etc.) about themselves or about other people. Students may not use school computers for commercial purposes or political lobbying.

## **Summary**

This is a list of the more common things students, faculty and staff are specifically **NOT** permitted to do.

- Download any files, especially music and videos, from the Internet.
- Use any form of “instant or private messaging” software on student devices.
- Install any applications or software onto Dodge County Schools’ computers.
- Disable or modify any running tasks or services.
- Transfer and/or store music files from any personal devices to Dodge County Schools systems.
- Play games, unless directed to by an instructor or supervisor for educational purposes, at any time on Dodge County Schools computers, including Internet-based games.
- Use proxies or other means to bypass the content filtering systems in place and/or defeat any settings that prevent the access of material deemed and flagged as inappropriate by the blocking devices.
- Use remote accessing software or hardware to take control of any network attached device or workstation.
- Remove License decals or inventory control tags attached to the systems.

- Disrupt its use by other individuals by connecting to other Dodge County Schools networks to perform any illegal or inappropriate act, such as an attempt to gain unauthorized access to other systems on the network.
- Anyone who inadvertently accesses an inappropriate site must immediately leave the site and report it to his/her instructor or supervisor.
- Attempt to log onto the network as a system administrator.
- Any user identified as a security risk may be denied access to the network.
- Damage caused by the intentional misuse or vandalism of equipment will be charged to the person who committed the act.
- Any damage to the student Chromebook/or device is the responsibility of the user.

## **Consequences**

Use of school's internet is a privilege. Failure to abide by the terms of this policy will result in the following disciplinary actions:

- Willful damage of computer hardware, computer software (including the deletion of programs and/or files) and computer networks will result in the student being responsible for the current repair and replacement cost of the damaged software and/or equipment. Any student violating the terms of this document will receive appropriate disciplinary action as defined by the school administrations.
- Students could lose computer/network privileges, and/or receive detention, suspension or expulsion.
- The Director of Technology or his/her designee may close an account at any time as required. The administration, faculty and staff of Dodge County Schools may make a request to the Director of Technology or his/her designee to deny, revoke or suspend specific user accounts based upon violations of this policy.

## **Improper Use and Content**

Users may not use the Dodge County Schools Network for purposes of harassment, intimidation or bullying of others.

Bullying is the repeated use of a written, verbal or electronic expression, physical act or gesture, or any combination thereof, directed at another student that:

- Causes physical or emotional harm to the student or damage to the student's property;
- Places the student in reasonable fear of physical injury or of damage to property;
- Creates a hostile environment at school for the student;
- Infringes on the rights of the student at school; or,
- Materially and substantially disrupts the education process or the orderly operation of a school.
- A hostile environment is a situation in which bullying causes the school environment to be permeated with intimidation, ridicule or insult that is sufficiently severe or pervasive to alter the conditions of the student's education.

Cyber-bullying involves an act of bullying through the use of technology or any electronic communication, including but not limited to electronic mail, internet communications, or instant messages. Cyber-bullying also includes the creation of a web page or blog in which the creator assumes the identity of another person; or, the knowing impersonation of another person as the author of posted content or messages, if the creation or impersonation creates any of the conditions described in the definition of bullying. Cyber-bullying also includes the distribution by electronic means of a communication to more than one person or the posting of material on an electronic medium that may be accessed by one or more persons, if the distribution or posting creates any of the conditions described in the definition of bullying.

Dodge County Schools shall, in its sole discretion, determine whether such conduct violates this policy and any other policies of Dodge County Schools. Users must remember that material distributed through the Internet is public. On the Internet, there is no central authority, so each site is responsible for its own Users. Complaints received from other sites regarding any of our Users will be fully investigated, and disciplinary action may be taken as a result.

### **Social Networking Sites**

While Dodge County Schools respects the right of employees, students and families to use social media and networking sites, as well as personal websites and blogs, it is important that any such personal use of these sites does not damage Dodge County Schools' reputation, its employees, or its students or their families. Student use of social networking sites is prohibited on Dodge distributed technology devices. All users should exercise care in setting appropriate boundaries between their personal and public online behavior, understanding that what is private in the digital world often has the possibility of becoming public, even without their knowledge or consent.

Dodge County Schools strongly encourages all employees, students and families to carefully review the privacy settings on any social media and networking sites they use (such as Facebook, Instagram, Twitter, Flickr, LinkedIn, etc.), and exercise care and good judgment when posting content and information on such sites. If an employee has a community that extends to persons who are parents, alums, or other members of the Dodge County Schools community, she/he must exercise good judgment about any content that is shared on the site.

Additionally, employees, students and families should adhere to the following guidelines, which are consistent with Dodge County Schools' community standards on harassment, student relationships, conduct, professional communication, and confidentiality:

- Users should not make statements that would violate any of Dodge County Schools' policies, including its policies concerning discrimination or harassment;
- Users must uphold Dodge County Schools' value of respect for the individual and avoid making defamatory or disparaging statements about the school, its employees, its students, or their families;
- Users may not disclose any confidential information of Dodge County Schools or confidential information obtained during the course of his/her employment, about any individuals or organizations, including students and/or their families.

Dodge County Schools has a strong interest in promoting a safe and supportive learning

environment, as well as maintaining a positive reputation in the community. If the school believes that an employee's activity on a social networking site, blog, or personal website may violate the school's policies or otherwise may have a detrimental impact on the learning environment, the school may request that the employee or student cease such activity. Depending on the severity of the incident, the employee or student may be subject to disciplinary action. Dodge County Schools reserves the right to impose discipline, up to dismissal or termination, for any behavior on or off campus that Dodge determines may impair or negatively impact the reputation of the school.

### **Theft and Vandalism**

Users must acknowledge the use of the intellectual property of others. Users must treat information found electronically in the same way as information found in printed sources. Rules against plagiarism will be enforced. It is the responsibility of each User to comply with the terms and condition for the acquisition and use of software found on the Internet. Dodge County Schools will not allow the copying or storing of illegally acquired software. In this case, vandalism refers to deliberate attempts to damage the hardware, software, or information residing on Dodge County Schools Network or any other computer system attached through the Internet. Attempts to violate the integrity of private accounts, files or programs; the deliberate infecting of a computer with a "virus," attempts at "hacking" computers using any method, or other such actions shall be a violation of this Policy.

### **"Netiquette"**

Users must abide by accepted rules of network etiquette, including, but not limited to, the following:

- Do not reveal personal information – your address or telephone number, or those of students or colleagues.
- Be polite. Do not be abusive in your messages to others. Use appropriate language and do not use vulgarities, or any other inappropriate language.
- Do not use the Dodge County Schools Network in such a way that would disrupt its use by others.

### **Waiver of Warranties; Limitation of Liability**

Dodge County Schools makes no warranties of any kind, whether express or implied, concerning this service. Dodge County Schools shall not be held responsible for any damages suffered, including the loss of data resulting from delays, non-deliveries, missed deliveries, service interruptions, or errors and omissions. Dodge County Schools denies any responsibility for the accuracy or quality of information obtained through this service. All terms and conditions as stated in this Policy are applicable to the use of computer resources at Dodge County Schools, in addition to internet use.

## **Preservation of Resources**

All resources are limited; computer resources are not an exception. Because space on disk drives and bandwidth across the lines, which connect Dodge County Schools Network both internally and externally, are limited, neither programs nor information may be stored on the system without the permission of the system administrator. Users are not to load software on any school computer. Each User is permitted reasonable space to store e-mail, Web, and personal files, as mandated by system file quotas. Dodge County Schools reserves the right to require the purging of files in order to regain disk space without warning. Users whose need for the resource is more pressing will have priority of space.

Employee Signature: \_\_\_\_\_