REVISED POLICY – PHASE IV TECHNOLOGY UPDATE – JANUARY 2018

UTILIZATION OF THE DISTRICT'S WEBSITE AND REMOTE ACCESS TO THE DISTRICT'S NETWORK

Parents, students, staff/employees and community members are encouraged to ~~A~~access ~~to~~ the District's ~~W~~website (_**www.celinaschools.org**_____)~~ is encouraged~~.

The following resources **are**~~shall be~~ available on the District's website:

(X) links to school websites

(X) School/District Departments

(X) the District's calendar~~ of events~~

(X) (gradebook program)

(X) (required State report)

(X) Board of Education agendas and minutes

(X) information concerning the District's Anti-Discrimination Policies and Procedures, including Section 504/ADA complaint procedures

(X) summary of all reported bullying incidents (updated twice a year)

(X) required Forms

(X) employment and Volunteer Opportunities

(X) resources for additional information during an crisis/emergency situation

(X) contact Info

( ) _____ **[e.g., School Choice Options]**

( ) _____

~~The Board encourages employees, p~~**P**arents, students, **staff/employees** and community members **should** ~~to~~ check the District's website regularly for changes to these resources and for the addition of other resources. Some resources may require a user name and password, or a login procedure due to the personally identifiable nature of the information provided through that resource (e.g., the gradebook program and e-mail system). If a user name and password, or log~~o~~in procedure, is necessary to access a resource, **the user should contact the applicable school or department for access.**~~information shall be provided on the website explaining who is eligible for a user name and password, how to obtain a user name and password, and detailed instructions concerning the login process.~~

Access to the District Network Through a Server

[NOTE: Please choose one (1) of the following options.]

OPTION #1

[x] Board members

[xx] District employees

[x] Students

(x) , as well as

(x) contractors,

(x) vendors,

(x) agents

of the District,

are not permitted to use their personally-owned or District-owned computers or workstations

(x) and/or web-enabled devices of any type

to remotely (i.e. away from District property or facilities) access the District's server and connect to the District's ~~N~~network.

[x] Any exceptions to this policy must be approved in advance, in writing, by the Superintendent/**Technology Coordinator**.

[END OF OPTION #1]

Option #2

[ ] Board members

[ ] District employees

[ ] Students

( ) , as well as

( ) contractors,

( ) vendors,

( ) agents

of the District,

are permitted to use their personally-owned or District-owned computers or workstations

( ) and/or web-enabled devices of any type

to remotely (i.e. away from District property and facilities) access the District's server and thereby connect to the District's ~~N~~network. This policy is limited to remote access connections that are used to do work on behalf of or for the benefit of the District, including, but not limited to, reading or sending e-mail and reviewing District-provided intranet web resources **( ) and completing assigned coursework**.

Each individual granted remote access privileges pursuant to this policy must adhere to the following standards and regulations:

( )~~A~~ his/her ~~device~~ computer/device must have **active on it**~~, at the minimum, the~~ **an** anti-virus **program with the latest updates from the manufacturer**~~software specified in the District's standards for remote access and connection~~

( )~~B.~~ the individual may only access the ~~N~~**n**etwork using his/her assigned user name and password

The individual **is prohibited from** ~~must not~~ allow**ing** other persons, including **friends and** family members, to use his/her user name and password to log**o**~~i~~n ~~in~~to the ~~N~~**n**etwork. The user may not go beyond his/her authorized access.

( )~~C.~~ his/her device may not be connected to any other network at the same time s/he is connected to the ~~N~~**n**etwork, with the exception of personal networks that are under the complete control of the user

~~D.~~ ~~the individual may not access non-District e-mail accounts (e.g. Hotmail, Gmail, Yahoo, AOL, and the like) or other external resources while connected to the Network~~

( )~~E.~~ his/her device may not, at any time while the individual is using remote access to connect to the ~~N~~**n**etwork, be reconfigured for the purpose of **connecting to another (an additional) network**~~split tunneling or dual homing~~

( )~~F.~~ use of the ~~N~~network**, whether connected directly or remotely,** is contingent upon the individual abiding by the terms and conditions of the ~~District~~**Board**'s ~~Network and Internet~~**Technology** Acceptable Use and Safety polici**es**~~y~~ and guidelines

[ ] **Users are required to sign the applicable agreement form (Form 7540.03 F1 or Form 7540.04 F1) prior to being permitted to use remote access.**

[ ] Additional standards and regulations for remotely accessing and connecting to the District network shall be ~~developed and~~ published in AG 7543 - Standards and Regulations for Remote Access and Connection.

Any user who violates this policy may be denied remote access and connection privileges.

[END OF OPTION #2]

Any employee who violates this policy may be disciplined, up to and including termination; any **(x)** contractor **(x)** vendor **(x)** agent who violates this policy may have his/her contract with the District terminated; and **(x)** any student who violates this policy may be disciplined up to and including suspension or expulsion.