Connect

5700 West Canal Road
Valley View, Ohio 44125

Telephone: 216-520-6900
Fax: 216-520-6969

1885 Lake Avenue
Elyria, Ohio 44035

Telephone: 440-324-3185
Fax: 440-324-7355

URL: www.ohconnect.org

System and Network Security Policy
Internet User Guidelines and Policy

Reviewed: June 1, 2018

This page intentionally left blank

CONNECT
System and Network Security Policy

Data maintained by Connect is the property of the school district or other customer which entered such data or to which such data is assigned. As a custodian of customer data, Connect is concerned that unauthorized use of such data be prevented. Accordingly, Connect has developed the following policy to maintain the integrity of customer data, to promote system security, to permit authorized access to data, and to prohibit unauthorized access.

I. DATA ACCESS

Access to customer data shall be available as follows:

A. Customer Personnel

1. The Superintendent, or Chief Executive Officer or school's equivalent of a Connect customer shall have read-only access to all customer data. The Treasurer or Chief Financial Officer shall have full access to fiscal data and read-only access to non-fiscal data.
2. Other employees of a Connect customer shall be granted access to said customer's data with the authorization of the customer's Superintendent, Chief Executive Officer, Treasurer, Chief Financial Officer or school's equivalent as appropriate. Authorization for access must be provided in writing, preferably on the Connect provided user request form.
3. The Superintendent, Chief Executive Officer, Treasurer, Chief Financial Officer, or school's equivalent may designate an individual, or individuals, with authority to grant access to the customer's data.
4. Customers may restrict (to the extent practical and technically possible) access to certain datasets and/or specific access types.
5. Connect shall provide each customer with a request form for the purpose of granting user access.

B. Connect Personnel

Connect employees shall be granted access to customer data if such access is necessary to carry out their assigned duties, but only for the purposes of maintaining data structure, researching and correcting problems, and providing back-up capabilities.

C. Third Parties

1. Third parties shall be granted access to customer data only when authorized in writing by the Superintendent, Chief Executive Officer, Treasurer, Chief Financial Officer, school's equivalent or their designee. A "third party" is defined as any individual or group of individuals not employed by customer or Connect.
2. Detailed staff and financial data and aggregate student data shall be transferred to the Ohio Department of Education, as authorized and/or required by applicable laws and regulations.
3. Access to hosted software by the software developers will be provided by Connect for support purposes.

D. Data Release Policy

Upon termination and/or expiration of a service agreement, the District shall be responsible to Connect for any and all costs associated with data conversion and/or transmission of district data on a time and materials basis. Connect will provide an estimate of the costs to complete the data conversion and/or transmission at the time that notification to terminate the service is given by the district. The district shall issue a purchase order to Connect in the amount of the estimated data conversion/transmission costs and all outstanding debts and obligations per Connect service and membership agreements as appropriate.

i. All written notifications shall be provided by the district via postal or electronic mail.

ii. The district shall provide a schedule of data transfer, specifying the dates, type of data/system transfer, and points of contact for the entity designated to receive the data.

iii. The district superintendent or CEO shall provide notification with permission to release student data adherent to the schedule of data transfer. No proxy may act on behalf of the district superintendent.

iv. The district treasurer or CFO shall provide notification with specific permission to release financial data adherent to the schedule of data transfer. No proxy may act on behalf of the district treasurer.

v. Connect shall make a good faith effort to adhere to the schedule of data transfer without delay or impediment no later than ten business days following the district's request, unless otherwise specified and agreed upon by Connect. Said transfer may be subject to constraints, related to and dependent upon the transferring and/or transferred agency and pertaining to staff availability, unexpected technical or system issues, and/or other unanticipated situations that arise.

vi. To protect the validity of the data, access to the Connect system subject to transfer shall be denied once the data transfer has been initiated.

vii. A system back-up of all transferred data will be maintained by Connect for a minimum period of 30 days. Should a district require access to or a re-transfer of data during said period of time, additional fees may apply.

II. DATA SECURITY PROCEDURES

The local network of users is the first point of security in the Connect network. To enhance security and reduce the risk of unauthorized access, Connect requires that the following procedures be followed:

A. Each user will be assigned one unique account for access to the network.

B. Each user account must have a password containing at least 8 characters. The password shall be treated as confidential information by the user. The user is responsible for protecting the confidentiality of his or her password, other access protocols, as well as customer and Connect information, in whatever form. Neither Connect nor any Connect customer shall maintain a list of passwords.

C. Each user and "Captive" accounts (accounts which have access to only limited, non-system programs and commands) are required to change their password if there is evidence of compromise of the authenticator.

D. A yearly report of fiscal accounts will be generated and provided to the customer's Treasurer, Chief Financial Officer or school's equivalent for review and signoff.

E. Users are responsible for ensuring that their workstations, (including, but not limited to terminals, Chromebooks, tablets, phones, and personal computers), when not in use, are properly logged off the system.

F. A user shall be granted only those privileges that are consistent with the duties and responsibilities of his or her position. Authorized privileges shall be categorized as "normal" or "extended". "normal" privileges will be granted when a user logs onto the system, and they represent those privileges required for the performance of the user's normal duties. "extended" privileges are those privileges which the user may be authorized to use, but which must be specifically enabled by the user before being utilized.

G. Access to the Connect network via an electronic network outside the Connect area will be restricted to the minimum level of access necessary for authorized users. No "general access" accounts shall be maintained.

H. Access to privileged or system accounts shall be granted only upon authorization of the Connect Executive Director, Connect Assistant Director, Business Services, or Connect System Administrator. Upon completion of outside access to a privileged account, the account password shall be changed to prevent further access without authorization by Connect.

I. OECN_SYSMAN privileges to any state software shall be granted only upon written request from the Superintendent, the Chief Executive Officer, Treasurer or Chief Financial Officer of a customer, and such request must state the purpose, length of time needed, and the employees who shall be granted such access. Connect shall not be responsible for such customer's files during the specified time period. Connect will not modify or make corrections to the customer's files, but will serve only in an advisory capacity.

J. Audit alarms shall be used to track attempts to break into a user or system account, as well as other attempts to breach security. Connect shall review the audit log for suspicious entries on a daily basis, and such entries shall be filed for future reference.

K. For security reasons, each customer must inform Connect immediately of any employee of such customer who has been terminated or has voluntarily left the employment of such customer. The accounts and files of such an employee shall be disabled and deleted within five business days.

Each customer must notify Connect immediately of any employee who has been placed on leave of absence, or short-term or long-term disability. Such an employee's account shall be disabled and re-opened only at the request of the employee's immediate supervisor.

L. In order to maintain the integrity of production data and software Connect may create test, demonstration and “play” datasets with user accounts as necessary and appropriate. A user request form for creation of non-production accounts is not required. Access to non-production datasets shall be granted to individuals consistent with the duties and responsibilities of his or her position for testing and training purposes.

In all events, the Executive Director, Connect Director, and designated Connect Staff shall have the authority and responsibility to take all actions necessary to ensure the integrity of data and the security of the computer system and to enable users to utilize the computer system as authorized.

III. NETWORK SECURITY POLICIES

A. Open Ports on Connect's Firewall/DMZ

Connect administers the firewall that protects all of the systems within the educational entities served by Connect from the Internet; Connect is responsible for creating open ports for access to systems within the network. Open ports create an inherent security risk for the specified system and subsequently other systems within Connect's Network. Open ports could allow systems to be compromised by malicious entities on the Internet. Once a system is compromised, since that system is already behind Connect's firewall, the reality exists for that system to be used to attack other systems in other school buildings without firewall protection.

All outside access shall be denied at the firewall. However, if a District or school wishes to have access from the Internet to a node in their network, a release form shall be signed authorizing the creation of an open port. The individual signing the request form states that they understand the risks and the District or School assumes the responsibility to secure the system and to accept the liability for any resulting damages caused through this open port.

Connect reserves the right to disable an open port if it is determined that said open port has been compromised.

IV. E-MAIL FILTERING POLICIES

A. SPAM filtering

Connect administers the flow of e-mail from the Internet to the schools within the network. Connect has facilities to block e-mail messages categorized as SPAM and/or unacceptable. Any effort to reduce the amount of unwanted e-mail messages will result in the loss of some legitimate e-mail messages. Connect's Staff will make every effort to minimize the number of legitimate e-mail messages that are blocked by the filter(s).

B. Virus filtering

Connect has facilities to block e-mail messages containing computer viruses. E-mail messages containing computer viruses will be blocked to prevent computer viruses from infecting the Connect network.

Connect's systems will filter all inbound e-mail served by Connect's internal e-mail servers. Connect's systems will also filter all inbound e-mail messages served by non-Connect e-mail servers. Any District or School that does **not** want e-mail filtering enabled for their own internal e-mail servers must provide written authorization to bypass filtering signed by the District Superintendent or by the Non-Public School Administrator, as appropriate.

V. INTERNET CONTENT FILTERING POLICIES

A. Content filtering

Customers that that choose to administer Internet content filter provided by Connect for their school, or school district, must designate those individuals the district authorizes to block and/or unblock access to specific Internet websites. Content filter administrators have the authority to bypass the filtering service provided by Connect. Individuals granted this authority also assume the responsibility for their actions as administers of the Internet content filters.

Connect
Internet User Guidelines and Policy

The Connect communication network provides access to computers and people all over the world. Along with this access comes the availability of material, which may not be considered to be of educational value within the context of the school setting. While it is impossible to control all materials on a global network, Connect has taken precautions to restrict access to potentially inappropriate materials. The guidelines below are designed to prevent inappropriate use of the Connect network.

I. INAPPROPRIATE USES

The Connect network shall not be used in any inappropriate ways or for any inappropriate purposes as determined by Connect system administrators. Inappropriate uses include, but are not limited to, the following:

A. Placement of unlawful information, computer viruses or harmful programs on the system, whether in public or private files or messages.

B. Unauthorized alteration of system software.

C. Transmission of any material in violation of state or federal law or regulation (including but not limited to copyrighted material, material protected by trade secret, and threatening or obscene material).

D. Use of obscene, vulgar, threatening, abusive, defamatory or otherwise objectionable material or language in public or private files or messages. No one shall use any Connect resource to obtain, view, download, store, forward or otherwise access any such material or language.

E. Use for personal business, for-profit activities or commercial transactions, unless authorized in writing by Connect in advance.

F. Use for employee recruiting (except posting of available positions by school districts), securing employment, product advertisement or political activities.

G. Use of another user's password or account.

H. Any use that violates another user's privacy, including without limitation, disclosure of such user's password, personal address, phone number or social security number.

I. Any use that interferes with use of the network by others or that degrades system performance.

Connect
Internet User Guidelines and Policy

II. POLICY

The user's use of the computer network and Internet is a privilege, not a right. A user who violates this Policy, shall at a minimum, have his or her access to the computer network and Internet terminated, which Connect may refuse to reinstate indefinitely. A user violates this Policy by his or her own action or by failing to report any violations by other users that come to the attention of the user. Further, a user violates this Policy if he or she permits another to use his or her account or password to access the computer network and Internet, including any user whose access has been denied or terminated. Connect may also take other disciplinary and punitive actions including pursuit of civil and/or criminal charges against individuals and/or organizations that violate this policy.

Use of the Connect network is limited to its registered account holders. Each account holder is responsible for any use or misuse of his or her password and/or account. While the network is intended for the private use of Connect's account holders, it is not guaranteed to be private. Connect reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. Connect system administrators will determine whether any use of the network is inappropriate or unauthorized, or whether any material or language is objectionable. Connect's decision will be final.

A teacher must closely supervise students using the Connect network at school. Parents or guardians shall be responsible for supervising students' use of the network outside school.

Use of any information obtained through the Connect network is at the user's risk. Connect specifically denies any responsibility for the accuracy or quality of such information.

Connect does not make any warranties, express or implied, including without limitation any warranty of merchantability or fitness for a particular purpose, with respect to the network, its services or features. Furthermore, Connect shall not be liable for any special, incidental, indirect, or consequential damages or for the loss of profit, revenue, or data arising out of any use of, or inability to use, the network, even if Connect shall have been advised of the possibility of the potential damage or loss.

Legal Reference: *Children's Internet Protection Act of 2000 (H.R. 4577, P.L. 106-554)*
Communications Act of 1934, as amended (47 U.S.C. 254[h],[l])
Elementary and Secondary Education Act of 1965, as amended (20 U.S.C. 6801 et seq., Part F)