LAKE GEAUGA COMPUTER ASSOCIATION

DATA SECURITY POLICY AND PROCEDURES

Data System Security Policy

The General Assembly and staff of Lake Geauga Computer Association (hereafter referred to as the Computer Center) recognizes that data maintained by the Computer Center is the legal property of the school district (hereafter referred to as the district) which entered such data or to which such data is assigned. Each district's individual portion of the Computer Center's computer which maintains district data is considered an extension of the district. The Computer Center, therefore, is a holder in public trust of the data.

The Assembly adopts the following policy statements concerning access to and security of the data. These statements are intended to assure the inviolability of the data, provide for procedures to permit authorized access to data and prohibit unauthorized release of data, and recommend features which districts and the Computer Center can implement to promote system and data security.

I. Data Access

Data maintained by the Computer Center shall be recognized as the exclusive property of the district. Each district shall be in control of its own data maintained at the Computer Center. Access to the data shall be granted as follows:

A. District Personnel

1. District personnel shall be granted access upon the written authorization of the District's Superintendent and Treasurer.

2. Such access may be restricted (as may be practical or technically possible) to certain data sets and/or specific access types.

3. The Computer Center shall provide a standard form for authorization.

B. Computer Center Personnel

1. Computer Center staff shall be granted access when such access is within the scope of their assigned duties, but only as may be necessary to maintain the data structure, research and correct problems, and provide backup capabilities.

C. Outside Access

1. Outside access shall be granted upon the written authorization from the superintendent of the district or his/her designee.

    a. "Outside" is defined as any individual or group of individuals not belonging to the school district or the Computer Center.

2. Data required to be transferred to the Ohio Department of Education shall be as defined by statute, State Board of Education Rule, and/or as outlined in the Education Management Information System Definitions, Procedures and Guidelines.

3. Written confirmation of the outside access shall be forwarded to the district superintendent within 24 hours.

II. Data Security Procedures

The first point of security is access to the computer system and its data via the local network of users. To enhance security and reduce the risk of unauthorized access, the following guidelines shall be followed:

A. Users will be assigned one unique account for access to the system.

B. Each user account shall require a password with a minimum of 6 characters. This password shall be treated as confidential information by the users. Users are responsible to safeguard their passwords, other access protocols, and district and Computer Center information, in whatever form. No list of passwords shall be maintained by the Computer Center or the District.

C. All users will be required by the system to change their password or at least

every 90 days; "captive" accounts (accounts which have access to only limited, non-system programs and commands) must have their passwords assigned by the Computer Center and shall be changed at least every year.

D. A review of user account activity will be performed quarterly by the computer staff. User accounts that have not been accessed in the previous 180 days will be disabled; users not accessing their account in the previous 90 days will be notified that such inactivity may cause their account to be disabled. Users should ensure their terminals, when not in use, are properly logged off the system.

E. Users shall be granted only those privileges consistent with the duties and responsibilities of their position. Authorized privileges shall be grouped in a "normal" and "extended" category: "normal" privileges are granted by the system when a user logs onto the system and represent the privileges required to perform the users normal duties; "extended" privileges are those privileges which the user may be authorized to use, but which must be specifically enabled by user before being utilized.

F. Access to the computer system via an electronic network outside the Computer Center area will be restricted to the minimum level of access necessary for authorized users. No "general access" accounts shall be maintained.

G. Access to privileged or system accounts shall only occur with the authorization of the Computer Center Director. Following outside access to a privileged account, the account password shall be changed to prevent further access without the Computer Center staff's knowledge.

H. Audit Log

Sufficient audit alarms shall be enabled to track attempts to break into a user or system account and other security related events. The audit log shall be reviewed daily for suspicious entries and shall be filed for future reference.

I. Notification by district users

1. For security reasons, each district should immediately notify the Computer Center if an employee has been terminated or has left the district. The accounts and files of the employees shall be disabled immediately and deleted within five business days.

2. Each district should notify the Computer Center when any district user is placed on leave of absence, or short-term or long-term disability. The user's

account shall be completely disabled and re-opened only at the request of the user's immediate supervisor.

J. In all events, the Director of Computer Services shall have the authority and responsibility to take actions necessary to insure the integrity of the data and security of the computer system, or to enable authorized district users to utilize the computer system to fulfill the duties associated with their positions.

K. The data security policy and procedures shall reviewed annually.

L. Current District Personnel Authorization List Attached.