ALLIANCE OF SCHOOLS FOR COOPERATIVE INSURANCE PROGRAMS

ASCIP

# Key Control Guidelines



Revision as of February 12, 2021

# PURPOSE OF KEY CONTROL

The purpose of this policy is to provide appropriate [electronic card key and[1]] metal key access and enhance security to district facilitieswhile maintaining oversight of the number of keys issued to employees.

# ISSUANCE OF KEYS

Routine access to locked district facilities or other secured areas within those facilities that are required for the performance of an employee's assigned duties will be provided through the issuance of appropriate keys to allow entry.

1) The [facilities manager/principal] has immediate responsibility for the issuance of metal keys and maintaining logs and records of all keys issued for access to district facilities. [If applicable, the [human resources department] has immediate responsibility for the issuance of electronic card keys and for maintaining log and records of access cards provided for those facilities in which a computerized magnetic locking system has been installed in accordance with approved procedures.]
2) Keys may be issued to district employees only upon authorization by a responsible department head and approval by the [facilities manager/principal, human resources department, and/or security manager]. The districts should only use keys that are part of **patented keying systems**.[2] Any disputes on the issuance of keys are resolved by the [superintendent/deputy superintendent of business operations].
3) Persons to whom keys are issued assume full responsibility for the security and proper use of keys issued to them. Key recipients must agree in writing that they shall:
   a) not lend or otherwise permit any keys issued to them to be used by any unauthorized person,
   b) not duplicate or alter the key and may not allow others to do so,
   c) report the loss or theft of any key within 24 hours to the [facilities manager/principal], [security manager], and their immediate supervisor, and
   d) return the issued key(s) to the [human resources department] upon relocation, reassignment, retirement, or termination of employment. (The [human resources department] will not certify clearance forms for individuals terminating employment until all keys issued to the employee have been returned.) Keys may not be sent through the U.S. mail or courier; they must be delivered in person. Keys must also be turned in to the [facilities manager/principal] for office relocation.
4) If applicable, appropriate fees approved by the [superintendent/deputy superintendent of business operations] will be assessed for damage, loss, or failure to return an assigned key for replacement of an assigned key. Additionally, rekeying costs also may be assessed for each lock affected by a lost or unreturned key. (Do we want the members to list the fees here in so way or fashion?)

[1] In the event a district uses electronic card keys, insert this additional verbiage. Electronic card keys provide additional security since they are more difficult to identify or duplicate with respect to specific key usages.

[2] In such systems, key blanks cannot be copied since they are protected by utility patents which make it illegal for third parties to produce keys that will work in patented locks. (Keys stamped "*Do Not Duplicate*" are not sufficient.) As a result, only locksmiths who are under contract with patented key manufacturers have access to their blanks. If employees try to copy patented keys, they cannot simply visit their local hardware store.

# CONTROL OF KEYS

1) The [facilities manager/principal] is the final authority to approve the issuance of a building master and/or area submaster key(s) [or electronic card keys], allowing full access to a school facility or storage area. Note that master keys should be issued- at the highest access level, on a per-site or per building (for larger facilities) basis and not on a grand master key basis covering all district buildings. Such limitations on the key scope will help avoid rekeying an entire district should a grand master key be lost or stolen.
2) Responsible department heads are authorized to issue, with the approval of the [facilities manager/principal, human resources department, and/or security manager], individual office or room key(s) [or electronic card keys] for employees.
   a) A key request memorandum or email must be properly approved and submitted to the [facilities manager/principal] when requesting a metal key. When issued, the employee must personally sign for the key.
   b) No more than one key for a particular lock will be issued to an individual. Special exceptions may be granted upon written approval by the [facilities manager/principal].
   c) The authorizing department head is responsible for:
      i) initiating requests for metal keys to be issued to employees in their department,
      ii) maintaining current, accurate records of all metal keys approved by him/her,
      iii) ensuring keys are returned when the employee no longer needs the key(s) or terminates employment,
      iv) verifying reports of lost or stolen keys with the [facilities manager/principal] within 24 hours of discovery of theft or loss,
      v) recovering applicable rekeying costs when employees lose or do not return issued keys upon termination and rekeying is determined necessary, and
      vi) preventing the installation of door locks that have not been approved by the [facilities manager/principal].
   d) The [facilities manager/principal] is responsible for:
      i) approving the issuance of building master keys or area submaster keys allowing full access to district facilities,
      ii) approving 24/7 full access or other type of typical access,
      iii) maintaining a keying system that provides security and convenience to departments occupying district facilities,
      iv) maintaining current, accurate key control records and issuing reports of keys issued as required, and
      v) acting promptly upon reports of the loss or theft of all keys to ensure appropriate investigation and determination of security risks.
   e) The key recipient is responsible for:
      i) using issued key(s) to gain access only to authorized area(s) to conduct district business and for the safekeeping of all district keys in his/her possession,
      ii) storing keys in a locked storage cabinet when not in his/her possession. Unmarked filing cabinets, desk drawers, and lockers are not considered to be secure storage areas for district metal keys [or electronic access cards],
      iii) ensuring the door(s) to a keyed assigned work area is properly locked or otherwise secured at the conclusion of work,
      iv) returning issued keys to the [facilities manager/principal] that are no longer needed due to relocation, reassignment, retirement, or termination of employment,
      v) reporting lost or stolen keys to the [facilities manager/principal], as prescribed in this policy, within 24 hours of discovery of loss or theft, and
      vi) paying for the replacement of lost keys or keys not returned upon transfer or termination of employment and for possible rekeying required by negligent loss of keys.
   f) [The [human resources department] is responsible for:

i) approving the issuance of electronic card keys,
ii) maintaining a secure electronic database to support an electronic card key system for district facilities,
iii) providing individually encoded electronic access card keys that provide access to selected facilities for authorized individuals, and
iv) acting promptly upon reports of the loss or theft of electronic card keys to ensure maintenance of facility security.]

3) **Penalties for Unauthorized Key Use**. Any person who knowingly makes, duplicates, possesses, uses, or allows a person not authorized to use keys for entry of district facilities or rooms without the appropriate authorization will be subject to administrative disciplinary action and may be criminally prosecuted under the laws of the State of California.

## LOST OR STOLEN KEYS

The loss or theft of metal [or electronic card] keys must be reported within 24 hours of discovery of the loss or theft to the [facilities manager/principal, human resources department, and/or security manager], the immediate supervisor, and the administrator who originally authorized issuance of the key[ or card]. Individuals issued the lost or stolen key(s) shall be responsible for paying the applicable replacement fees. Replacement metal keys will be issued only after submission of a new key request authorization form and payment of applicable fees. Fees for unreturned keys, including lost and stolen keys, and for replacement of keys [or cards] shall be as approved by the [facilities manager/principal].

Districts should also consider RFID-based key control systems. Such systems have sensors in the keys that enable districts to pinpoint the location of each key in real time.

### Rekeying

Generally, the rekeying of rooms, secure cabinets, and/or buildings will be required whenever metal keys are lost or stolen if the [facilities manager/principal and/or security manager], after analyzing the circumstances associated with the loss or theft, determines that security of the affected facility or storage area has been compromised. In such cases, the individual to whom the key was issued and/or the department head that authorized issuance of the key may be held responsible for the costs of the rekeying. Decisions to require rekeying at departmental expense may be appealed to the [facilities manager/principal].

Departments may also unilaterally request rekeying of locks by submitting a written request justifying the requirement for rekeying to the [facilities manager/principal]. Rekeying is not considered routine maintenance and the department requesting rekeying normally will be charged for the work.

# TEMPORARY AND EMERGENCY KEYS AND ACCESS

### Knox-Boxes®

Fire Department key boxes such as the Knox-Box Rapid Entry System are used for secure building emergency access by first responders. Knox-Boxes allow entry into a building without forced entry damage or delay. The district can store a master building key [elevator keys, access cards, and floor plans] in a Knox-Box mounted near each building's entrance. Each Knox-Box is keyed to a single master key controlled by the local responding fire department.

To get a fire department key box, the [superintendent/deputy superintendent of business operations] should discuss Knox-Box use and procedures with your local fire department. Determine the items needed to be stored in the key box for each building as well as the locations to mount the key boxes. Generally, Knox-Boxes are mounted on strong, outside walls with reasonable 24/7, all-weather access, are no higher than 6 feet off the ground, and are near obvious fire department entry locations as determined with the assistance of your local fire department.

Contact your local fire department if the district desires to implement, secure, or change its Knox-Box use. If your keys or emergency contact persons are changed, inform your local fire department as soon as possible.

### Vendor and Contractor Keys

Temporary metal [or electronic card] keys may be issued to outside vendors and contractors that need after-hours access to limited, necessary district facilities when no other alternative is available. Such access must be approved by the [facilities manager/principal and/or security manager] upon submission of a written justified request by the appropriate authorized administrator of the department or office accepting responsibility for supervising use of the temporary keys. Following terms outlined in its agreement, vendors and contractors are required to pay rekeying costs when their access period expires. Vendors and contractors must also acknowledge that funds may be retained from payments due the vendor or contractor to reimburse the district for costs associated with rekeying the affected area(s) and property losses stemming from lost keys.

### After-Hours or Temporary Access

When a department or office requires access to district facilities during periods other than normal working hours, arrangements can be made to have the facility or area opened. The department or office must provide adequate advance written notification to the [facilities manager/principal and/or security manager] for arrangements to open and close the facility. The department will arrange with the [facilities manager/principal and/or security manager] to assign an overtime guard to control access to the facility. The department is responsible for providing an account to pay the overtime personnel.

Employees may access district facilities, including the parking areas, after hours, on weekends, or holidays as long as they possess their employee badge [electronic card key] and display it upon request by the guard on duty. For safety reasons, employees upon arrival, shall ~~make~~ contact and inform the security guard of their presence and upon their departure.

### Guest and Visitor Access

Guests and visitors to district facilities are not normally issued temporary keys. Customary guest and visitor sign-in, badge, ~~and~~ escort procedures and requirements apply, and district employees with keys will provide entry into locked facilities and areas as appropriate on an "as needed" basis.