Denver Public Schools Access Control Policy and Procedures

Purpose

To safeguard our students and DPS community members while also facilitating access to public facilities, space and equipment by authorized users (faculty/staff, students and affiliates), DPS has established a policy on access control. This policy and supporting guidelines set out specific responsibilities, conditions and practices that are designed to address critical access needs in a manner which minimizes risks and maximizes the protection of the district's physical assets and private information

Policy Statement

The safety and security of the district's physical space and assets is a shared responsibility of all members of the Team DPS. To meet this obligation, the district has established access-control policies and procedures to address the design, administration and management of access-control systems and measures to ensure their integrity and consistency in implementation. Access-control privileges are determined and assigned by central and school-based leaders, and the Department of Safety and Security based on the specific needs and requirements of the district and the key/card holder.

Employees

All school district employees are required to wear DPS-issued ID badges with the photo side visible in plain view for others to see while in any school district building or on school district grounds. Full-time, part-time and substitute employees will be issued an ID badge at the beginning of their tenure with the district. There is no charge to the employee for the badge. Employees who fail or refuse to wear an ID badge may be subject to disciplinary action.

Access to school buildings during any school breaks or holidays is set at the discretion of each individual school's principal. Authorization to educational buildings must be requested by the employee for any access during days other than that of the scheduled work week.

ID badges and key fobs allowing electronic access into DPS facilities must be utilized for access to buildings instead of keys except in emergency situations. ID badges are property of the school district and the responsibility of individual employees to safeguard. ID badges are not to be defaced, modified or duplicated in any way. ID badges are not to be loaned or transferred to any other person. Any missing, lost, or stolen ID badges and key fobs must be reported to DPS Safety and Security Dispatch ***immediately***. DPS Dispatch will deactivate the card in order to prevent unauthorized access to DPS facilities and safeguard members of the DPS community.

In the event that any ID badge or key fob is lost, stolen, or destroyed, the first replacement badge or key fob will be free of charge. ID badges that are no longer usable due to wear shall be replaced at no cost. ID badges and key fobs must be returned to the DPS supervisor or Human Resources when employment is terminated.

Visitors

All visitors to the School District shall display a temporary visitor ID badge while they are in any School District building or on School District grounds during school hours. Upon entering a school building, visitors shall report to the school office to register and receive a temporary visitor ID badge. These badges will not allow either interior or exterior access to the facility. Visitor badges must be worn at all times while the visitor is in a DPS-owned facility. Visitor badges must be returned to the main office upon check-out. Visitors who do not comply with this Policy will be escorted from the property. School staff members who observe visitors without proper identification are requested to escort the individuals to the main office immediately.

Contractors and Vendors

All contractors and vendors are required to sign in at the main office of the DPS facility they are visiting and obtain a visitors badge. Contractors and vendors must sign out at the main office and return the visitors badge when leaving the DPS facility.

All contractors and vendors working regularly in a DPS facility or facilities over a period of at least 30 days are required to wear temporary DPS-issued ID badges with the photo side visible in plain view for others to see while in any School District building or on School District grounds. Contractors and vendors will work with the DPS employee overseeing their contract to obtain a DPS-issued ID badge. Completion of the DPS Card Access and Authorization form is required prior to an access badge being issued. Contractors will be required to account for all ID badges issued to their employees with their sponsoring DPS employee every three months. Contractors should collect any DPS-issued ID badges from employees immediately upon termination of employment. The DPS sponsoring employee is responsible for ensuring contractors are aware of badging procedures and that the contractors which they are responsible for maintain badges at all times.

Access for any persons other than those employed directly through Denver Public Schools (DPS) must fill out and sign “Third Party Access Card Agreement” and return to Safety and Security. Access cards will not be administered to contractors until form is filled out, signed, and returned.

ID badges are property of the School District and the responsibility of individual contractors to safeguard. ID badges are not to be defaced, modified or duplicated in any way. ID badges are not to be loaned or transferred to any other person. Missing lost or stolen ID badges or key fobs must be reported to DPS Safety and Security Dispatch ***immediately***. DPS Dispatch will deactivate the card in order to prevent unauthorized access to DPS facilities and safeguard members of the DPS community.

In the event that any ID badge or key fob is lost, stolen, or destroyed, the first replacement badge or key fob will be free of charge. ID badges that are no longer usable due to wear shall be replaced at no cost.

ID badges must be returned to the school district personnel office upon completion of the contract and/or project. If contractors or vendors fail or refuse to wear an ID badge on DPS property, their contracts or agreements with the district will be subject to review and possible termination.

Access-Control Approval Process – Levels of Approval

All access requests (keys, fobs, electronic access cards), must be made through an approved liaison with the Department of Safety and Security. A person requesting access must meet the applicable criteria and complete the access request form with signed approval from the school or department leader.

Any employees with multiple cards MUST return all but one card to Safety and Security: 900 Grant St, Room 114. Once all extra cards have been surrendered, all requested access can be added to one single card once

authorization has been received by the parties' direct supervisor/department head.

There will be five (5) levels of approval that any request can fall under. The level of access control approval for any area is determined by the level of risk and exposure. The following levels of approval will apply to all access requests:

Level 1 – Most basic level of approval; single door or exterior door access within normal business hours.
- Department head, manager, or designee will approve and process access control requests.

Level 2 – Network and critical areas within a building – building access within normal business hours.
- Network closets approved by Technology Services or manager for critical area will approve access control requests.
- Will enter approval queue and require approval before processing.

Level 3 – Building access (exterior doors) outside of normal business hours.
- Will require approval from the school administrator if for a school site or from Department of Safety and Security if non-school site.

Level 4 – Access to multiple buildings.
- Will require approval from instructional superintendent for schools or Chief of Safety and Security for non-school sites.

Level 5 – Access to all DPS facilities twenty-four hours per day, seven days per week.
- Will require approval from Chief of Safety and Security.

Vendors – Access level will depend on the type of access required by scope of work.
- Long term vendors will have a one-year expiration date but will be audited quarterly.

New Employees

If an employee is new to DPS, the following procedure must be followed:

- Employee's department or HR liaison will process all necessary information through the HR system in order for new employee to obtain a badge/electronic access card.
- Employee's department liaison must submit a work order request to activate that employee's interior/exterior access.

Separation or Transfer

Employees:

Separation – It is the responsibility of the immediate supervisor or human resources representative to collect all access devices (metal keys, badge/electronic access card, proximity devices, and temporary cards) issued to an individual at the time of separation. The direct supervisor/school principal will then:

- Consult with the Department of Safety and Security to ensure that all ID badges or key fobs are accounted for or deactivated prior to separation.
- The direct supervisor is responsible for initiating a request to DoTS to terminate all network access in the system.
- The direct supervisor must forward all collected access devices to the Department of Safety (900 Grant St, Room 114) and Security within 24 hours of collection, to enable proper and timely verification and deactivation.

Transfer - If an employee is transferring to a new department, facility, or level of responsibility requiring access

beyond normal business hours, or to a new or additional district building, the following procedure must be applied:

- Employee's current direct supervisor must submit a request to deactivate that employee's interior/exterior access.
- Employee's new direct supervisor will then request the activation of the employee's new interior/exterior location.

Access-Control Policy Violations

The following acts are examples of violations of the access control policy:

- Defacing, modifying, or duplicating an ID badge
- Loaning or transferring ID badges
- Defacing, puncturing, or otherwise modifying a key fob or access card
- Loaning keys
- Utilization of physical keys to access a DPS-owned facility except in emergency situations
- Damaging, tampering or vandalizing any district lock or access control hardware
- Propping doors open
- Admitting unauthorized person(s) into the building
- Failure to return a key when requested or upon leaving the employment of the District
- Failure to report missing key(s), ID badge(s), or key fob(s)

Law Enforcement/Emergency Services

The Denver Police Department (DPD) will be issued sufficient number of key fobs to be assigned to all DPS squad cars. DPD will work with DPS Safety and Security to record and track key fobs assigned to DPD squad cars. In addition, an access card will be located in the Knox box designated for first responders and emergency services personnel at each DPS facility. In the event that a DPD-assigned key fob is missing, lost, or stolen, DPD will inform DPS Safety and Security immediately.

Access Control Policy Department/Facility Liaisons

Department and/or Facility Access Control Liaisons must complete the DPS prescribed training for the access control system and successfully pass a minimum assessment prior to utilizing the access control management software system. Authority levels within the software management system will be determined and assigned by the Department of Safety and Security.

Panic Alarm Notification System (Duress button)

Each DPS facility is equipped with a Panic Alarm/Duress button located in the main office of each building. In case of emergency, this button can be utilized to initiate a building-wide lockdown or full lockdown. The duress button should not be used in a situation requiring modified lockdown.

When pressed, the duress button will automatically alert DPS Safety and Security Dispatch, lock doors installed with access control, and initiate an announcement over the building public address system. The duress button will only lock doors with access control installed. Doors without access control will still need to be locked manually.

In the event of an emergency requiring utilization of the duress button, building staff should immediately follow

the lockdown procedures in section 3.7 of the DPS Emergency Response and Crisis Management Manual, including notifying DPS Dispatch and 9-1-1 by telephone if at all possible. The Site Administrator/Principal (or their designee) is the **only** person authorized to **order** a **release** from a lockdown, in consultation with DPS Safety and Security, Police Department, or the Fire Department.

Intercom Systems and Visitor Management

Most DPS facilities utilize an intercom or, in some cases, a visual intercom to assist with visitor management. It is the policy of DPS that the person responding to the intercom signal **MUST** interact with the person who has pressed the intercom button requesting entrance to the building. At no time should a visitor be admitted to the building without such verbal interaction.

When responding to a request for entrance from a visitor using the intercom, the DPS staff person responding to the request should ask for the visitor's name and purpose of the visit. In cases of camera-integrated intercoms, even if the visitor is known to the DPS staff person, the staff person will still request that the visitor state the purpose of the visit. Once the visitor has responded, the DPS staff person will inform the visitor that the door release has been activated and they may enter the building. The DPS staff person allowing entrance will ensure the visitor proceeds to the main office to sign in and obtain and visitor's badge.