Access Control Program
Framework and Standard Operating Procedures

1.0 Background: The Purpose and Goals of Access Control

The purpose of Portland Public School's (PPS) Access Control Program (ACP) is to secure the property and assets of PPS from theft or damage and to maximize the safety of our students, staff and members of the PPS community, while providing equitable access to District property for those legitimately requiring it.

The goals of the Program are to ensure that:

- The appropriate level of access control are provided for all PPS buildings and assets;
- Access control is provided comprehensively and equitably across school campuses and meets the needs of our students, staff and the community;
- Access control installations and ongoing maintenance of access control systems are delivered in an effective manner;
- Appropriate control of keys and access cards exists to protect the overall integrity of the Access Control program; and
- An overall framework is in place for the ongoing management of access control that establishes institutional standards and sets forth responsibility and accountability at appropriate levels.

2.0 Definitions

Key is a device inserted into a lock that allows the lock to be disengaged mechanically, thereby permitting access to a building or interior area that is otherwise locked.

Access Control System refers to locking system that is hard-wired, consists of hardware and software, and stores information in two places, in a computer server and in a local control panel.

Card Activated Locking Mechanism refers to a programmable locking device that requires power to operate (wired or battery), is activated by a card with a magnetic stripe, and may have a key override.

Access Card, Card Key, Access Key Fob are examples of items used to disengage an access control locking mechanism, thereby permitting access to a building or interior area that is otherwise locked.

Designated Authority is the functional responsibility held by the full-time employee designated by the head of the faculty administration or department to be responsible for authorizing access to buildings or interior spaces controlled by the faculty administration or department. The Designated Authority holds oversight responsibility and accountability for Access Coordinator functions. In a school setting the Designated Authority is generally the school principal.

Access Coordinator is the functional responsibility held by a full-time employee assigned responsibilities of key control, requisition, distribution, retrieval, and record keeping within the school or department. The Access Coordinator is also assigned responsibilities of coordinating access card requirements of administrators, teachers, students and employees of the District. The Access Coordinator is the liaison between the school/department and Security Services or Facilities. This position is generally held by a school secretary or clerk.

3.0 Standards

Standards and procedures shall be established to guide the installation and maintenance of mechanical and other locking systems as well as access control systems in all PPS buildings. These shall address fixtures, structural, electrical and other requirements and stipulate that all installations on District property

comply with all applicable PPS policies, municipal, provincial and federal laws, standards and codes. The Department of Facilities & Asset Management shall be responsible for establishing such standards and procedures that support the purpose and goals of the Access Control Program. All new construction and renovations to existing space will conform to these standards, which shall be applicable until modified by PPS or rescinded.

4.0 Responsibility and Authority

The Chief Operating Officer shall be responsible for prescribing PPS standards and procedures for the control of interior building spaces. The functional responsibility for leading and overseeing the PPS-wide management of building access control shall reside with Security Services and Facilities Operations.

Security Services

Security Services shall:

- Have responsibility for electronic access arrangements for all campus buildings;
- Undertake periodic audits to monitor for effectiveness and compliance;
- Manage the card access software.

Security Services shall hold the authority to activate access cards – and to delegate this authority to Facilities Operations as required or appropriate—by setting up restricted local capabilities in the department, division or operating unit to issue cards (card keys or fobs) and program access.

The Director of Security Services is the designated security expert and approval authority in all security installations on PPS property, including locks and keys, access control systems, video surveillance and alarms systems, etc. The authority for approving access to more than one building on the same access card, card key or access key fob shall be held by the Director of Security Services or designee.

Facilities Operations

Facilities Operations, has the overarching custodial responsibility for the physical upkeep, maintenance and servicing of all aspects of PPS facilities and grounds, including interior building spaces. Facilities Operations has the authority to access all interior areas for the purposes of fulfilling this overarching responsibility and to the extent necessary to do so, liaises with occupant units and Security Services.

Facilities Operations shall be responsible for all physical installations in PPS buildings that restrict access to locked space. This includes, but is not limited to:

- Ensure that a common template for managing key control processes (e.g., issuance, collection, inventory, security, record-keeping, etc.) is implemented by every faculty administration, department, division or operating unit;
- Responsibility for the maintenance and repair of doors, frames, locks, keys, door and frame hardware, electrical and fiber optic cabling, and access control hardware and devices (e.g., proximity reader, electronic strike, door contacts/magnets, electronic latches, power transfer hinge, motion sensor, etc.).
- Responsibility for central key production, issue, control of master keys, and distribution of regular/change keys to the Designated Authority or Access Coordinator.
- Responsibility for keeping of up-to-date records of:
  a) Great Grand Master (GGM), Grand Master (GM) and exterior master key holders across the District;
  b) Keys manufactured for and given to faculty administration, departments, divisions and operating units to control.

The Director of Facilities Operations (or equivalent/designate) shall monitor the issuing of master keys and shall, from time to time, undertake an audit of all master key types (GGM, GM & Exterior Master), including those held by all PPS faculty administration, departments, divisions and operating units, and shall provide the audit report to the Director of Security Services for dissemination to the proper authority.

Faculty Administration or Department

Responsibility and accountability for the control of interior building spaces and providing access to those spaces rests with the building administration or departments that have been assigned those spaces through the PPS's formal process of space planning and allocation. The building administration or departments shall undertake this "control" in compliance with standards and procedures established in this document. Within the building administration or departments there shall be a Designated Authority charged with the functional responsibility of access management and key control. The Designated Authority shall be responsible for maintaining detailed records of names of individuals who are key holders and the specific keys being held. The Designated Authority shall also be responsible for maintaining records, of those to whom access has been provided to using the "Key Check-out form" provided in this document.

Card access to the building will be provided during the following times:

- Principals, vice-principals, maintenance, custodial, senior administrators: all hours, all days
- Teachers and other school staff: 6:30 am – 8:00 pm during the school year during normal working days. Card access during weekends, down-days, breaks, and holidays will not be provided. Access to the school can be granted through the use of the CUB permit process.

Variations from the above times will need to be approved by the Designated Authority and Security Services.

5.0 Compliance with Technical Standards

No area of the District shall be secured except by a locking device authorized by the Facilities & Asset Management Department. Exceptions may be granted by the Director of Facilities Operations on an individual basis.

6.0 Designated Authorities

A Designated Authority shall be named in every school or department to have overall responsibility for access management and key control. The Designated Authority has the authority to request changes to locks, is responsible for deciding who gets access within the building and ensures the Access Coordinator functions are enacted, as applicable.

The **Access Coordinator** function includes the following:

- Submits requests to the Facilities Operations for keys to be manufactured.
- Approves the issue of regular change keys for interior doors
- Receives and issues and retrieves keys.
- Maintains local records of key holders and key inventories, using the "Key Check-out form" provided in this document.
- Administers/coordinates keys for desks, cabinets, display cases, etc. in the faculty administration, department.
- As a matter of operational policy, undertakes an annual audit of keys controlled by the faculty administration or department.
- Approves requests for access cards, card keys or access key fobs for employees.

- Coordinates access needs of students and other constituents, and liaises with Security Services in regard to card issue and recovery, and IT system requirements.
- Issues and retrieves access cards locally, as appropriate or required.

7.0 Control and Distribution of Keys and Access Cards

Control and distribution shall be managed through a coordinated, multi-level system. The institutional key control function resides with Security Services and Facilities Operations which shall establish operating procedures relative to the issuing of keys. Local keys are managed by the Designated Authority of the school or department.

The framework for controlling and authorizing the issuance of keys is presented in the "Levels of Key Access" chart below.

Keys

Normally, a Sub-Master, Grand Master, or exterior key shall be issued only to Principals, Vice-Principals, and Custodians unless otherwise approved by the Director of Security Services.

Access Cards

As with keys, access to multiple doors to offices, facilities or buildings shall be programmed only on access cards (or card keys or access key fobs) held by those persons whose District responsibilities require it and where the issuance of multiple cards would be impractical or redundant.

Record Keeping

A record of approval for each key and access card issued shall be maintained by the Access Coordinator in a format consistent with the record keeping procedures established by Security Services and Facilities Operations. Reference the "Key Check-Out" form attached to this document

Key and Access Card Retrieval

The Designated Authority shall be responsible for ensuring that keys and access cards are returned to the Designated Authority or Access Coordinator when it is no longer appropriate to possess them. Staff members will sign out keys at the beginning of each school year and sign them back in at the close of each year or at the time of termination of their assignment at that building. Access provided through an access card should be blocked systematically as early as possible (e.g., date of employee departure or transfer, end of the academic session of appointment or enrollment, etc.). The Access Coordinator is responsible for notifying Security Services in the event that card access needs to be altered.

Procedure for Lost or Stolen Keys or Cards

In the event of a lost or stolen key, the Access Coordinator shall be responsible to submit a Key Replacement Form to Facilities Operations.

The Designated Authority of the school or department that issued the key shall be notified and shall decide about key replacement or possible lock/cylinder change. Facilities Operations and the Designated Authority shall together determine appropriate action should any type of master key be lost or stolen.

In the event of a lost or stolen access card, the Access Coordinator shall contact Security Services as early as possible. Security Services may arrange to block systematically all building access programmed on an access card that has been reported lost or stolen by the employee.

Repair of Locks, Keys, Card Readers, Door Hardware

Facilities Operations shall be solely responsible for repairs or modifications to locks, doors and associated hardware. Only technicians authorized by Facilities Operations may repair or replace any portion of an access control system. All calls for assistance should be directed to Facilities Operations at 503-916-3303 during PPS business hours or the "On-Call" phone, 503-730-9682 evenings and on weekends.

Facilities Operations Staff

Facilities Operations shall establish strict internal Standard Operating Procedures that restrict the use of PPS building keys to times and purposes related to the Department's overarching custodial responsibility for the physical upkeep, maintenance and servicing of interior building spaces. Permanent assignment of keys to Facilities Operations staff shall be made only in cases of demonstrated need for operating, safety and security reasons.

Outside Contractors

Contractors who require keys or access cards to do work on campus will make arrangements through the Project Manager or Maintenance Manager who hired them. A master key shall not be issued to a contractor unless warranted by exceptional circumstances and authorized by the Project Manager who shall arrange close scrutiny of its use until returned; and only where a release form has been signed by the contractor to deduct funds from its contract to cover the cost of re-keying the building or part of the building if the key is lost or stolen. The Project Manager in charge of the work shall be responsible for securing this signed document, copies of which shall be provided to the Director of Facilities Operations (or designee) and/or the Director of Security Services (or designee).

Where an access card is required, the Project Manager or Maintenance Manager shall make arrangements with Security Services and Facilities Operations and shall provide a precise schedule of dates and times for activation and de-activation.

Access cards are issued to an individual and shall never be given to anyone else to use. The card access system logs via computer each time a card is presented for access. Giving an access card to someone other than the authorized user may result in that access card being disabled and the user's card access privileges revoked.

- It is the responsibility of the employee issued the access card to **immediately** notify the Access Coordinator. The Access Coordinator shall notify Security Services and their Designated Authority of a lost or stolen access card.
- It is mandated that badges be displayed at all times when in the work environment.
- Access Card Holders who habitually forget their access card, or who fail to report their access card lost may be referred to their supervisor and may be subject to discipline.
- Requests to vary from this policy will be sent in writing to Facilities Operations.
- Use of access cards for any non-official purpose is strictly forbidden. Any person utilizing access cards for any illegal or prohibited purpose may be subject to disciplinary or legal actions.
- Access Cards remain the property of the PPS and must be surrendered when requested.

Levels of Key Access

Exterior Keys

Room Types	Key Types			
	Master	23 or 25 [2]	Change	Gate Key
Specific exterior doors key [1]		X	X	
All exterior doors key	X	X		
Key Cabinet (Located in main office) [8]		X		
People issued these keys	Principal, Head/Lead Custodians	FOMs, PMs, Security, Maintenance	Only staff approved by Director of Security	Coaches, Principals, Maintenance, Custodian

Interior Keys

Room Types	Interior						
	GGM	GM	17 [2]	X	IT [2]	PGE [7]	Change
Main Office	X	X	X				X
Classrooms & Offices [3,4]	X	X					X
Classroom Storage [3,4]	X						X
Gymnasium, Cafeteria, Auditorium, Media Center [5]	X	X		X			
Staff RR	X	X		X			
Work room/staff lounge	X	X		X			
Storage Rooms	X	X		X			
Custodian Office	X	X	X				
Custodian Storage Rooms	X	X					
Boiler room	X	X	X		X		X
Mechanical rooms	X	X					
IT/Electrical Closet (HDF/MDF)	X	X			X		
Sensitive Storage (i.e. Records Room)	X						X
People issued these keys	Principal, Head/Lead Custodians	Vice Principal, Custodians	FOMs, PMs, Security, Maintenance	Teachers, Staff, Specialty Programs	IT Staff	PGE as req'd	Staff and Programs as applicable

[1] In schools without card readers, one exterior door shall be keyed such that there is a unique key to it to be given to those needing access to this specific school.

[2] These keys are district-wide keys and are to be keyed the same as all other schools in the district. All other keys are unique to each school. Boiler/Custodian offices vary in access per school whether an exterior or interior key type

[3] These keys are to be unique to each room (i.e. each classroom/office door is unique to that specific classroom/office and any storage within that classroom/office if of the same key type)

[4] The kitchen and kitchen storage and office(s) as well as gym storage and office are to be keyed similar to being its own classroom/office/storage use

[5] The gymnasium, cafeteria, auditorium, and media centers are to be treated as common staff spaces

[6] Special Program defined as contractors and others that run programs in our schools, but are not PPS staff (i.e. the Sun Program)

[7] In some schools, PGE will require access to one electrical room from the exterior. In this case, their access should be a unique key

[8] Keys within key cabinet should provide access to all spaces within the school

KEY REPLACEMENT FORM

It is the requirement and the responsibility of the individual to whom keys are issued to report all lost or stolen keys to the Access Controller for your building/department/school. Stolen keys must be reported immediately.

School:_____   Date:_____

Employee Name:_____   Signature:_____

Missing Keys were: ☐ Lost   ☐ Stolen

Key(s) provide access to what area(s):

_____

_____

Describe the circumstance under which keys were lost or stolen:

_____

_____

Access Coordinator Name: _____ Signature:_____ Date:_____

Designated Authority Name:_____ Signature:_____ Date:_____

Form is to be faxed to PPS Maintenance at 503-916-3044

KEY CHECK-OUT FORM

SCHOOL/DEPARTMENT	DESIGNATED AUTHORITY	KEY COORDINATOR

STAFF NAME	AREA ACCESSIBLE	KEY NUMBER	DATE OUT	STAFF SIGNATURE	DATE RETURNED	KEY COORDINATOR INITIALS	NOTES

KEY AGREEMENT

I understand that key and access card control is a matter of workplace safety, ensuring building security and minimizing potential for loss or theft of property. As such, I agree to use assigned keys and/or access cards for official Portland Public Schools (PPS) purposes only. I agree to maintain assigned keys and/or access cards in a secure and responsible manner. I will not allow an unauthorized person to use keys and/or access cards assigned to me. I agree that upon employment separation, I will return to PPS all keys that have been issued to me.