Ortonville Community Historical Society Building Access Policy

Adopted by the OCHS Board of Directors on January 29, 2024

The Ortonville Community Historical Society takes proactive steps to protect the assets in its collection. We store the history of our community in our buildings, represented by both artifacts and documents. Most of these assets are one-of-a-kind artifacts with historical and sentimental value which cannot be replaced, even with insurance. The museum houses artifacts that are on loan from other museums, and we have a moral and financial responsibility to protect those pieces. Our buildings also contain modern assets with financial value, such as computers. Our ability to recover financial losses from insurance companies depends on our ability to demonstrate adherence to appropriate security measures.

The implementation and maintenance of strong security should be balanced with practicality; if the processes to provide appropriate accesses are too rigid, people will find a way around those processes that are detrimental to the overall goal. This policy describes the Building Access policy endorsed by the Board of Directors to provide that balance.

We reduce risk to these assets when we follow these principles regarding building access:

- Limit access to our campus buildings to “Minimally Necessary”
- Access to the buildings is controlled and monitored at the individual level – we know who has the authority to enter our buildings, and when access has occurred

The Old Mill Museum is equipped with an Access Control System that provides the ability to control access to the building at the individual level, including time-of-day and calendar restrictions. It provides reports summarizing when a user code has been used to access the building. We use these capabilities to support this policy. Access codes will be granted to individuals based on their current role in Museum operations.

The Board of Directors shall appoint a Security Administrator who will have these responsibilities:

- Understand the full operation of the Access Control System
- Program schedules in the Access Control System
- Create Access Codes for Users, and provide the User with their code with instructions on its use.
- Make adhoc decisions regarding issuing additional codes or non-standard access beyond the guidelines recommended by the Board
- As requested by the President, provide reports to the Board, including 1) Who currently has access, including day/time restrictions, and 2) Who has actually accessed the building.
- Monitor the Access Control System batteries and replace when necessary.
- Train a backup person who can take over in case the primary Security Administrator is unavailable.
- Store appropriate records to enable a backup person to seamlessly assume responsibility if required.

- Regularly review the list of authorized users, and update access when people change roles (for example, changes in office-holders due to elections).
- Regularly review the records of building access, and report unusual/suspicious activity to the President.

Guidelines

Role	Type of Code	Day/Time Restriction
President	Individually Assigned	24 hours, 7-days a week
Vice-President	Individually Assigned	24 hours, 7-days a week
Secretary	Individually Assigned	24 hours, 7-days a week
Treasurer	Individually Assigned	24 hours, 7-days a week
Trustee	Individually Assigned	24 hours, 7-days a week
Security Administrator	Individually Assigned	24 hours, 7-days a week
Member	Group (all use the same code)	During dates/times the building is otherwise open to the public
Cleaning Crew	Assigned to the Cleaning Manager	Limited to dates/times scheduled for cleaning
DPW	Physical Key Access	24 hours, 7-days a week
Others (as determined by the Security Administrator)	Follow the principle of “minimum necessary”	Follow the principle of “minimum necessary”

Responsibilities of Users:

- Do not share an individual code with others. In case of a security breach, it will be assumed that a code being used to access the building represents the person to which the code is assigned. Violations can result in the loss of your access privileges.
- Know that your access will show up on reports viewed by the Board of Directors
- Contact the Security Administrator if you think your code may have been compromised, or you need it changed.

Physical Keys

A limited number of physical metal keys are used by the Access Control system.

- One physical key shall be provided to the Ortonville DPW for their regular use in entering the building.
- Other physical keys shall be stored by the President and the Security Manager in secure locations outside the Mill, and shall not be used for regular access.