Recommended

WASHINGTON CENTRAL UNIFIED UNION SCHOOL DISTRICT

Board of Directors' Policy

BACKUPS

POLICY: F43

WARNED: _____

ADOPTED: _____

EFFECTIVE: _____

Individual User Responsibility: WCUUSD users must ensure that information that represents any part of a plan, system design, or that relates to the management of accounts are adequately protected from loss. District file servers and information stored in Google GSuite in the cloud are frequently backed up and archived; this is the suggested method for ensuring that information loss is prevented. If a user is unable to ensure adequate loss protection, they should contact the WCUUSD Information Technology Helpdesk (ithelp@u32.org) for assistance in resolution of this problem.

Not Responsible for Backups of District or Personal Data stored locally on devices: WCUUSD information systems are for official district use. Personal, non-school or work-related data should not be stored on district systems. WCUUSD will not backup user's district, school or personal data files or programs that are not stored on WCUUSD servers (or in the Google G-Suite environment) or have no relevance to WCUUSD business. Employees, Staff members, students, etc. who store personal, non-school or work-related data on their school devices do so at their own risk and expense. Examples include but are not limited to encoded music files, digital images personal pictures and games. The Information Technology Department may remove such items from WCUUSD systems at their discretion without prior warning to individuals.

General Storage Rules

- Maintain records in an appropriate storage form (i.e., Storage area network, network attached storage, paper, magnetic tape, microfilm, flash drive, optical disk) for the recommended length of time indicated by this policy.
- All records being prepared for storage should be described and include the following information on a label in order to facilitate their reference, review, and destruction:
    - The inclusive dates
    - Originating department name
    - Type of media
    - Date of destruction
    - Contact name and telephone number.
- Ensure the appropriate forms of records are complete and copies of such records can be reproduced in a complete and readable form upon request.
- Store all records in a manner that permits the efficient retrieval of stored records and the efficient return of records borrowed from storage.

- Restrict access to stored records to those individuals who have an appropriate need and permission to retrieve the records.
- Ensure all records are stored in a climate-controlled location with protection from hazards (i.e., theft, water, fire).
- Confirm that records copied onto an alternative storage medium (storage area network, network attached storage, microfiche, diskette, tape) are complete and readable before the original paper record is destroyed. All records stored in an alternate format must be available for reading and/or duplicating within a reasonable timeframe. Once records have been transferred, the original version can be destroyed according to this policy.
- Protect computerized data with password, code or card system.
- The Uniform Preservation of Business Records Act requires retention of general business records for three years from the creation of such records if no retention period is specified by regulation.
- Credit card transaction data should be stored only as long as required for financial tracking and auditing purposes. The specific credit card holder information such as the account number, expiration date, or other magnetic stripe information should never be stored in electronic format unless specific approval is received from the IT Department and the WCUUSD Policy Committee.