



Responsible Record Management Programs

Presented by: Suzanne Kennedy

Harris & Company ^{LLP}
harrisco.com
info@harrisco.com

Workplace Law
& Advocacy

1.

Record Management and Retention – Why is it important?



PowerSchool Data Breach

- Large quantities of student, parent and educator data
- Included historical records dating back decades
- Affected millions of individuals
- Retaining excessive data meant more sensitive information was exposed than needed



Accountability by Schools

Alberta and Ontario Privacy Commissioners

- Schools lacked policies and procedures
- Failed to have appropriate oversight of data PowerSchool maintained
- Failed to have controls that would support proper retention and destruction
- No privacy and security clauses in contracts



Toronto Zoo - Ontario IPC, 2025

- January 2024 Cyber Attack
- 10 days unauthorized access to networks
- 80 servers encrypted
- 1.2 million records placed at risk
- Employees, donors, guests and members of the public
- Data posted on the dark web



Findings

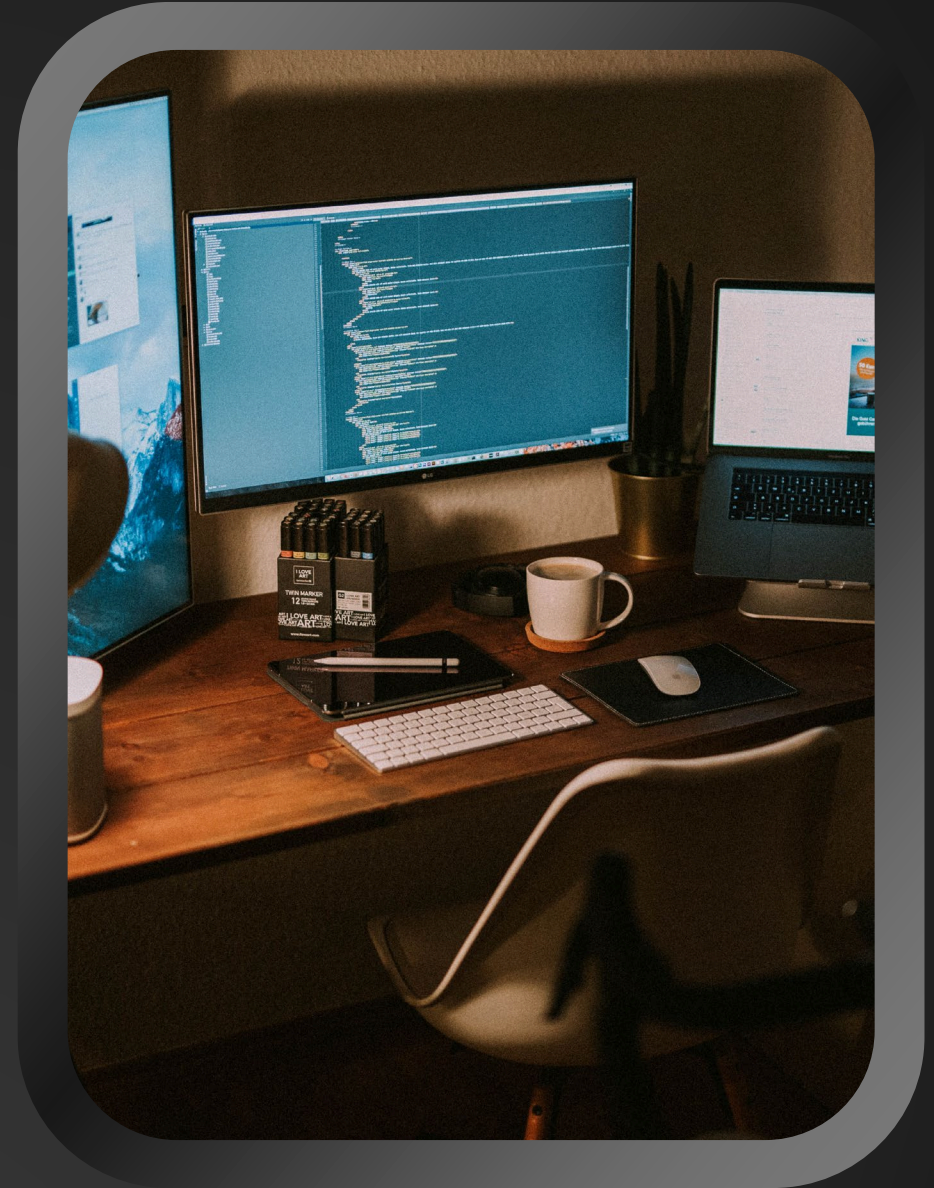
- IPC noted records kept well beyond applicable retention periods
- Visitor info kept for 20 years instead of 6 years
- Detailed employee records kept for lengthy periods
- No records management policy



What we are seeing- Other Record Retention and Liability Issues

In addition to broader legal exposure for over retention in the event of data breaches . . .

- Privacy complaints for unnecessary retention
- Failure to comply with statutory minimum retention periods
- Failure of trustees, directors, senior officials to exercise appropriate oversight and diligence
- Unavailability of evidence needed in litigation due failure to retain



2.

Record Management and Retention The Basics



Record Management for Schools

Four Pillars

- Legal Compliance
- Governance & Accountability
- Secure Retention/
Destruction
- Transparent Access Controls



Record Management Systems

Why it matters?



- **Efficiency** - Provide an organized system for managing records throughout their life cycle
- **Compliance.** Ensure information is retained in accordance with legal requirements
- **Consistency.** Ensures consistent security and retention standards with respect to all categories of records, whether digital or physical
- **Protects Organizational Interests.** Operations, institutional memory, litigation, accountability, audits, and planning



Governing Legislation

- School Act
- BC FIPPA/PIPA
- Employment Statutes
- Income Tax / CRA Bulletins



Student Records

Section 79

- A board must have written procedures for storage, retrieval and appropriate use of student records
- Ensure confidentiality of the information contained in student records
- Establish and maintain a record for each student and each child registered with the board.



Good and Prudent Practices

- Operational and Administrative Need
- Good Governance to Support Decision-making
- Accountability and transparency
- Protect against risk and legal claims



What's Important to Create and Keep . . .

- Records of decisions
- Evidence of due diligence
- Records you are required to maintain
- Records that may be needed to defend actions
- Records that form part of “institutional memory”
- Records needed for administration and operational purposes





Legal and Regulatory Requirements

Ensure compliance with minimum requirements

- FIPPA/PIPA – 1 year
- Permanent Student Record – 55 years
- Schedules, vacation, hours, payroll – 4 years
- Financial Records - 6 years
- Occupational health and safety records – varies

Non compliance can lead to complaints, legal exposure and reputational harms

Consider Limitation Periods

It benefits the school district to retain records that may be needed in defense of its operations and decisions

- 2 years standard limitation period in BC
- Subject to the “discovery rule”
- Ultimate limitation period 15 years
- Delayed for minors until they reach age of maturity
- Delayed for incapacitated adults
- No limitation for claims of assault, sexual assault, sexual misconduct





The Record Lifecycle

Creation or Receipt

Record is generated or received

Classification

Categorized by type and retention schedule

Active Use

Ready access required for operations

Archive/Inactive Storage Disposition

Sensitive records retained for compliance, operations, legal claims, reference

Disposition

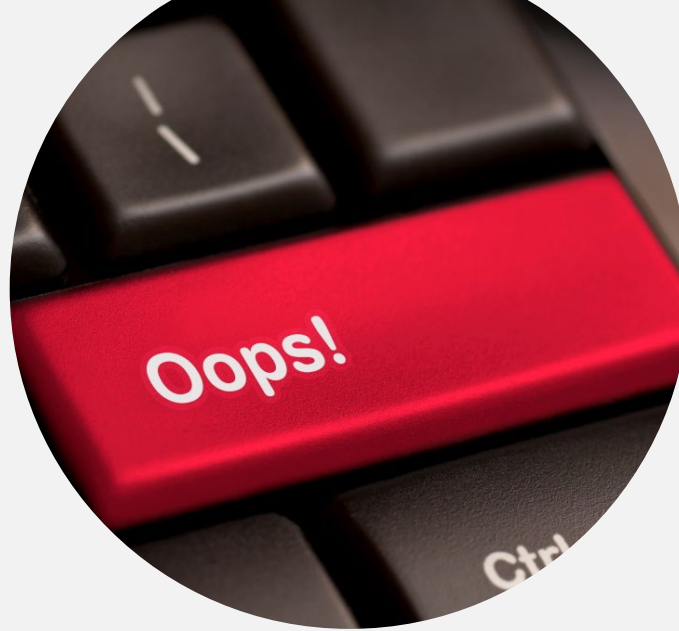
Secure destruction



3.

Data Security





Organizational, Technological & Physical Measures



Organizational Measures

- Need-to-know basis
- Policies
- Training
- Enforcement



Physical Measures

CONSIDER

- Security
- Devices control
- Access to devices
- Storage, destruction and retention

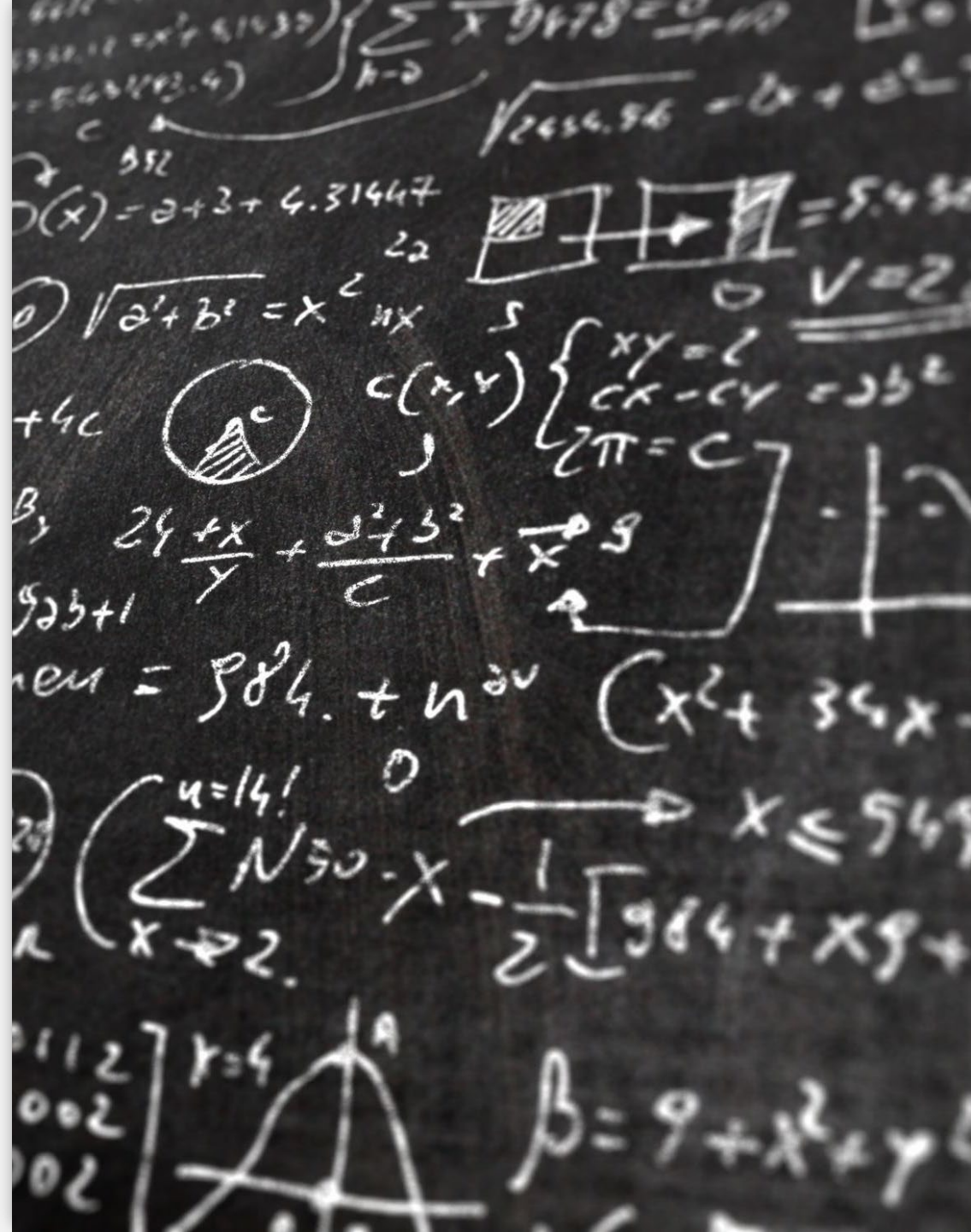


Technological Measures



The “Need to Know” Principle

- Personal Information should be shared internally and externally only on a “need to know” basis
- Files and data bases only accessed and used for work related purposes
- Avoid unnecessary discussion or disclosures





Contractual Measures and Third Party Providers



Managing Relationships with Third Party Vendors

- Importance of privacy impact assessments
- Assessing data sensitivity
- Reviewing contracts
- Data security standards
- Requiring legal compliance
- Maintaining accountability
- Keeping your options open

3.

School District Record Management



Policy

- Roles and Responsibilities
- Records Management Officers
- Securely Archiving Sensitive Materials (when not needed for routine operational purposes)
- Complying with Minimum Required Periods
- Transitory Records
- Secure Storage & Disposal
- Documenting Storage and Destruction





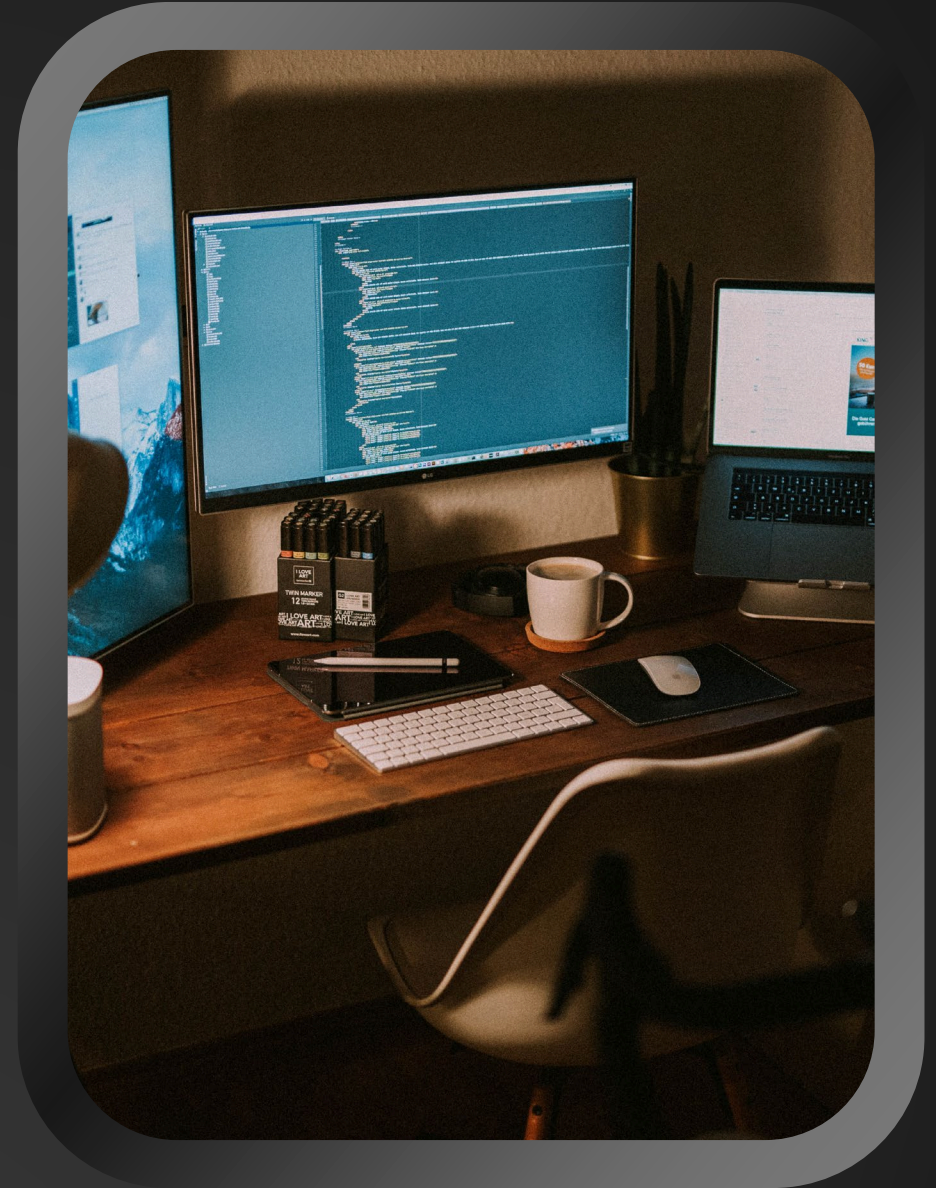
Record Retention Schedule

- Instructions
- Transitory Records
- Statutory Minimums
- Policy
- Retention Schedules by Category



Operationalizing the Schedule

- Appoint Records Management Officers
- Add categories as needed
- Consider recommended retention periods
- Develop systems for archiving – long term storage
- Create systems documenting destruction



Categories of Records Covered

- 1 Student Records
- 2 Administrative
- 3 Employment and HR
- 4 Contracts, Legal and Disputes
- 5 Governance and Policies
- 6 Planning and Operational
- 7 Financial
- 8 Facilities, Capital Projects
- 9 Information Technology and Privacy



CONFIDENTIAL

Active Period vs. Archived Period

- For sensitive records
- Secure storage when records no longer needed for day to day operational purposes
- Protection from cyber risks



Secure Storage Requirements

For sensitive records and personal information

- 1 Locked cabinets for physical files
- 2 Access limited to authorized staff
- 3 Password protection for digital records
- 4 Audit logs
- 5 Restrict storage on personal or mobile devices



4.

Transitory Records



What is a Transitory Record?

- Short term low value information
- Needed for only a brief period to complete a routine action or until a more permanent record can be found
- Not required for evidence, accountability, audit, legal or historical purposes
- Can be disposed of when no longer needed





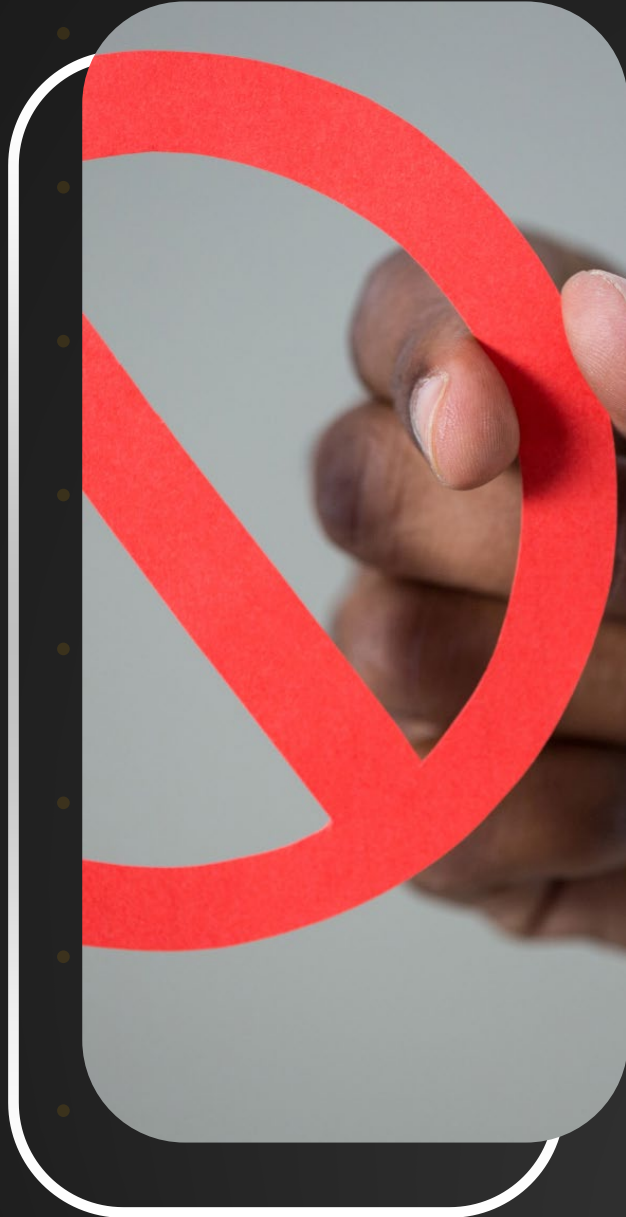
Characteristics

- Temporary usefulness
- Does not form part of official documentation of decision making
- Easily reproducible
- No long term operational, legal or fiscal value

Examples

- Meeting invites or emails scheduling meetings
- Drafts or working notes after a final version is approved
- Duplicate copies maintained for convenience
- FYI messages, reminders or clarifications
- Auto generated system notifications
- Spam invitations





What is NOT Transitory

- Original notes of meetings or interviews
- Final reports, decisions approvals
- Contracts, agreements or financial documents
- Records required by law, audit or retention schedules to retain
- Any working papers or materials needed to explain why or how a decision was made

Identifying Transitory Records

- **Consider:** Does this document support accountability and decision making?
- **Confirm:** Is this document the final or official copy?
- **Future Use:** Is it likely anyone will need this document in the future for evidence or reference purposes?
- **Verify:** Is the information captured elsewhere in a permanent record?



When to Dispose of Transitory Records

- As soon as the information is no longer needed
- When final version is approved and stored
- Once the task, meeting or transaction is complete





Why it Matters

- Reduces storage and clutter
- Improves efficiency
- Minimizing risk in audits, investigations or FOI requests
- Supports better knowledge management



5.

Secure Destruction



Why it Matters

- Prevent unauthorized access to personal or confidential materials
- Reduces legal, privacy and reputational risk
- Supports efficiency



What Secure Destruction Means?

- Records cannot be reconstructed or retrieved
- Applies to both physical and digital records
- Records are inspected before destruction to confirm no longer needed
- Destruction is documented
- Destruction can be verified and audited



Methods

PAPER

- Shredding (cross cut or micro cut for sensitive materials)
- Pulping
- Incineration

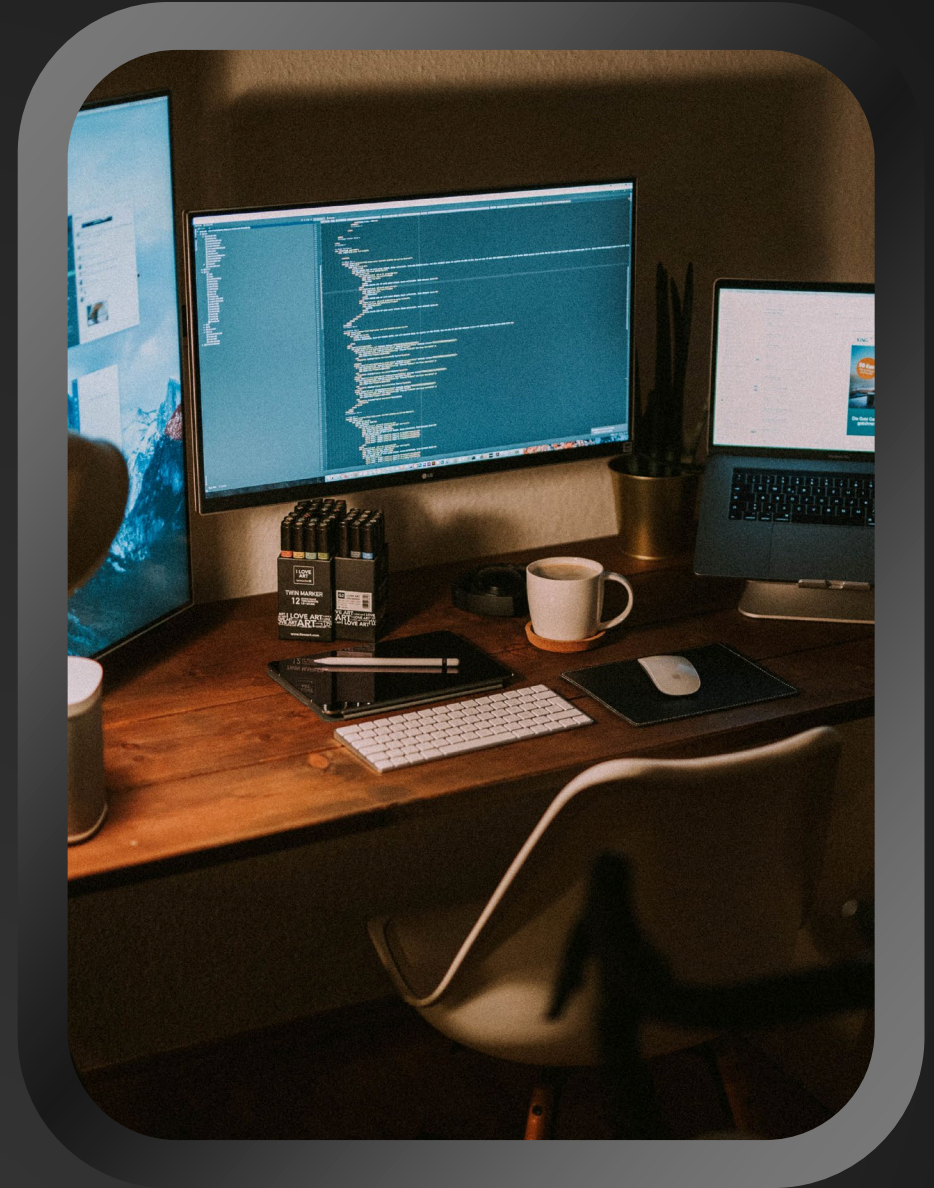
DIGITAL

- Secure wiping tools
- Overwriting
- Cryptographic erasure
- Physical destruction of storage media



Maintain a Destruction Log

- Record type or description
- Date of Destruction
- Method Used
- Person who authorized destruction
- Confirm review by destruction
- As for certificate, if using external vendors



Next Steps

- Review the Policy and Materials
- Support good security practices with staff
- Encourage secure storage
- Discourage over collection and retention
- Understand and comply with archiving recommendations
- Follow secure destruction practices



Role for School Based Administrators

- Review the materials
- Identify modifications
- Identify any other sensitive materials
- Consider and select methods of archiving
- Consider and select methods of destruction
- Review with program areas
- Appoint Record Management Officers
- Provide Instruction to Staff on the Policy



Questions?



Suzanne Kennedy
Partner
skennedy@harrisco.com

THANK
YOU