

EDMONTON PUBLIC SCHOOLS

January 14, 2003

TO: Board of Trustees

FROM: A. McBeath, Superintendent of Schools

SUBJECT: District Technology Specifications and Guidelines

ORIGINATOR: A. Habinski, Executive Director, School and District Services

RESOURCE

STAFF: Glenn Johnson, Bob Maksymic, Boris Oskin, Darwin Martin, Dale Tomas

INFORMATION

**Background**

The board policy on District Technology (KA.BP – Appendix II) was approved in April 2000.

District Technology has developed the technology policy framework in response to three needs identified by district staff:

1. In order to make wise decisions about technology, district staff needed consistent high quality advice.
2. It is more efficient and cost-effective when common technologies, applications and processes are used across the district. As the range of hardware and software widens, more resources are needed to acquire the technology, to support it and to train and retrain staff.
3. Specifications and guidelines need to become common operational practice rather than treated as a separate planning process.

The board policy is supported by several district Administrative Regulations and a series of technology specifications and guidelines. As part of an ongoing process, the technology specifications are developed and updated with representative input from our various stakeholder groups.

A diagram of the technology policy framework is attached (Appendix I), which shows the Administrative Regulations and Specifications that presently exist.

A new Administrative Regulation and three new specifications that have been recently developed are shown on the diagram as highlighted boxes.

*KD.AR: Security of District Technology*

District technology security refers to proactive and reactive strategies to protect the access, availability, integrity and confidentiality of district information systems, including hardware, software and data. The administrative regulation provides the framework for more detailed specifications and guidelines that apply to all central departments and schools. (Appendix III)

*2A: Computer Equipment Re-Use and Disposal Guidelines*

When disposing of surplus computer equipment, schools should consider its re-use as well as the environmental impact of disposing of the equipment in a landfill. Schools may choose to advertise the surplus computer equipment for sale on the Purchasing and Contract Services Web site or request Purchasing and Contract Services to assist with the disposal of the equipment. (Appendix IV)

*4D: District Applications Programmer Support*

Decision units responsible for district software applications must ensure that primary and backup programming staff are assigned to provide support for their systems. The backup programmer must have an acceptable level of technical skill and sufficient knowledge about the unit's business processes to respond effectively to requests for programming support. The specification includes recommendations made in the external auditor's report. (Appendix V)

*4E: Application Systems Documentation and Testing*

When buying, developing or altering district application software, the decision units responsible for the application must prepare the documentation and complete testing before the software is installed. The format and content of the documentation must comply with District Technology's Documentation Standards Template. As well, testing of district applications must follow the recommended processes outlined in this specification. The specification includes recommendations made in the external auditor's report. (Appendix VI)

All specifications and guidelines are posted on the District Technology website and changes are communicated via Superintendent's Memo.

GJ:gl

- Appendix I: Technology Policy Framework
- Appendix II: Board Policy KA.BP
- Appendix III: KD.AR - Security of District Technology
- Appendix IV: 2A - Computer Equipment Re-Use and Disposal Guidelines
- Appendix V: 4D - District Applications Programmer Support
- Appendix VI: 4E - Application Systems Documentation and Testing

## Appendix II

**CODE: KA.BP**  
**TOPIC: District Technology**

EFFECTIVE DATE: 25-04-2000  
ISSUE DATE: 26-04-2000  
REVIEW DATE: 04-2005

The board believes that the performance of all students and staff is enhanced through the appropriate use of technology.

### DEFINITION OF TERMS

Technology, in its broadest sense, can be defined as all tools and machines that have been developed to enhance human control over the natural and made environment. The focus of this policy, however, is on digital technologies that are used to enhance teaching, learning, communication, and information management including computer hardware, software, network communications and electronic information resources.

Reference(s):

[KA.AR](#) - District Technology Standards  
[District Technology Specifications and Guidelines](#)

**CODE: KD.AR**  
**TOPIC: Security of District Technology**

EFFECTIVE DATE:  
ISSUE DATE:  
REVIEW DATE:

### **A. DEFINITION OF DISTRICT TECHNOLOGY SECURITY**

District technology security refers to proactive and reactive strategies to protect the access, availability, integrity and confidentiality of district information systems, including hardware, software and data.

### **B. RATIONALE**

As the computing environment moves towards a more open architecture model, the district must establish a consistent approach to technology security. The wide area network in Edmonton Public Schools consists of several interdependent elements. Each element must be protected in order for the entire system to operate reliably and without interruption. District-wide security measures ensure uninterrupted access and prevent a variety of problems, including: loss of information, inappropriate access to confidential information, intentional or accidental destruction of hardware and software as well as system breakdowns in district applications such as student information, e-mail, payroll and human resources and the financial system.

The administrative regulation provides the framework for more detailed specifications and guidelines that apply to all central departments and schools. The regulation's specifications and guidelines define the controls necessary to ensure that legal and Freedom of Information and Protection Act (FOIP) requirements are met

### **C. PROCESS**

The specifications and guidelines under this regulation will address issues such as: appropriate use of technology by staff and students, control of access and use of encryption to secure district data, logging of Internet and e-mail usage, physical security of hardware, secure remote access, requirements for the use of the Internet and intranet, training and awareness of users and the disposal of surplus computers. As technology evolves, additional specifications and guidelines will be required in support of the integration of technology into our work.

Reference(s):

[KA.BP](#) – District Technology

[KA.AR](#) – District Technology Standards

[KC.AR](#) – Appropriate Use of District Technology

[District Technology Specifications and Guidelines](#)

[Freedom of Information and Protection of Privacy Act](#)

**2A: Computer Equipment Re-Use and Disposal Guidelines**

Effective Date: (draft)

Review Date: December 2004

Implementation Timeline: TBA

---

**SUMMARY:**

In order to safeguard information and to meet FOIP requirements, schools shall remove all data from computer hard drives prior to disposing of them. When disposing of surplus computer equipment, schools shall consider its re-use as well as the environmental impact of disposing of the equipment in a landfill.

Schools may choose to advertise the surplus computer equipment for sale on the Purchasing and Contract Services Web site or request Purchasing and Contract Services to assist with the disposal of the equipment.

In each case, schools shall comply with the guidelines established within this specification and should contact Purchasing and Contract Services for advice and assistance in the disposal of the surplus computers.

**RATIONALE:**

District principals have requested that guidelines be established to assist schools in the disposal of surplus equipment. In order to safeguard against the release of private and sensitive data and to meet the requirements of FOIP, it is essential that surplus equipment be disposed of in a consistent manner in all district schools and central services decision units.

Information processing equipment contains environmentally hazardous substances (e.g. mercury, cadmium) and therefore its disposal should be done in an environmentally friendly manner. Personal computers are comprised of more than 1,000 materials, many of which are highly toxic if released to the environment. Sending computers and other information processing equipment directly to the landfills could pose a serious threat to human health and our environment.

Edmonton Public Schools supports Alberta Environment's initiative: "Fluorescent Bulb and Computer Recycling Program". Under this program, local Alberta companies are certified to collect and process fluorescent bulbs and computers. Using these companies would support this recycling initiative.

**DEFINITIONS:**

Computers and any other information processing devices may be identified as surplus if:

- it is not economically advisable to invest in repairing the equipment; (e.g. obsolete parts, expensive memory cards)
- the equipment can no longer meet the needs of the school or the decision unit;
- it is part of the long-range plan for evergreening the information technology.

## **INFORMATION SAFEGUARD AND SOFTWARE LICENSES REQUIREMENTS:**

1. Schools and decision units are responsible for safeguarding information.
2. All equipment identified as surplus should be disconnected from the district and school networks.
3. All information from all hard drives must be erased without the ability to restore it. This includes:
  - all documents (e.g. word processor documents, spreadsheets, presentations)
  - all software including operating systems (e.g. Microsoft Office, Exchange, Windows, MacOS).
4. To ensure secure removal of information, computer hard drives should be overwritten by binary zeros (i.e. “wiping out hard drive” process). This should be done by a qualified computer technician. Schools or decision units may contact the ITS Help Desk for assistance.

## **PROCESS:**

1. Schools and decision units should contact Purchasing and Contract Services to assist in recycling or disposal of surplus information processing equipment.
2. Equipment identified as surplus will be posted on the Purchasing and Contract Services Web site for other schools or decision units. The minimum requirements for the resale of computers to district schools or decision units will be determined by ITS and Purchasing and will be changed from time to time. The current minimum requirements are:
  - Windows system: Pentium I or better, 166mhz CPU, 16 MB RAM, 1.2 GB hard drive, running Windows 95 OS;
  - MAC system: PowerMac 5500 or better, 225mhz CPU, 32 MB RAM, 2 GB hard drive, running MAC OS 8.
3. Equipment that is not wanted by district schools or decision units will be sold by Purchasing and Contract Services to outside organizations or offered to charitable or non-profit organizations. In such cases, original documentation pertaining to the computer system shall be transferred.
4. If there is no interest in the equipment, Purchasing and Contract Services will dispose of it in accordance with Alberta Environment regulations.
5. Schools and decision units are responsible for storing the surplus equipment until final disposal.

---

See also District Technology Specifications and Guidelines <http://dtp.epsb.net/standards.htm> and Computer Workstations for Staff Specifications <http://dtp.epsb.net/techstandards/3A.htm>

For Purchasing and Contract Services information see:

<http://purchasing.epsb.edmonton.ab.ca/products/computers/staffworkstations.cfm>

**4D: District Applications Programmer Support**

Effective Date: draft

Review Date:

Implementation Timeline:

---

**SUMMARY:**

Decision units responsible for district software applications must ensure that primary and backup programming staff are assigned to provide support for their systems. The backup programmer must have an acceptable level of technical skill and sufficient knowledge about the unit's business processes to respond effectively to requests for programming support. District Technology recommends that applications developed locally by DU's or schools for their own use also follow these guidelines.

District applications are defined as applications that are centrally supported and used in more than one DU or school. Local applications are those developed or purchased for use in a single DU or school.

**TIMELINE:**

Effective immediately, all district application systems (e.g. Student Information, BPS, FIS, QuickBooks, TRS and SNAP) must have primary and backup programming staff assigned to address the programming requirements.

**RATIONALE:**

In the absence of key programming personnel, the integrity and reliability of software applications can be compromised. Both District Technology and central DU's recognize that relying on one person to provide programming support for the system is a risk. Should the analyst be absent and the work assigned to another programmer, then the timeliness and accuracy of the service may not meet acceptable standards.

District Technology, in consultation with DU's, should assign backup resources for all key positions as well as assess and arrange for any cross training required.

**RESPONSIBILITIES:**

1. District Technology will maintain an inventory of all district application systems. The inventory will consist of the names of the decision units responsible for the applications, names of the support analysts, the location of the documentation, and schedules of planned releases.
2. The decision unit responsible for the systems will have a primary support programmer analyst assigned to their system.
3. The decision unit responsible for the systems will have a backup support programmer analyst assigned to their system.
4. The analysts' supervisor will identify the training requirements necessary to ensure primary and secondary programming support is in place.

**4E: Application Systems Documentation and Testing**

Effective Date: (draft)

Review Date:

Implementation Timeline:

---

**SUMMARY:**

When buying, developing or altering district application software, the decision units responsible for the application must prepare the documentation and complete testing before the software is installed. The format and content of the documentation must comply with District Technology’s Documentation Standards Template. As well, testing of district applications must follow the recommended processes outlined in this specification. District Technology recommends that applications developed locally by DU’s or schools for their own use should also follow these guidelines.

District applications are defined as software that is centrally supported and used in more than one DU or school. Local applications are applications developed or purchased for use in a single DU or school.

**TIMELINE:**

Effective immediately, all district applications in development must be documented and tested by District Technology and decision units before they are installed.

In cases where existing district applications are not documented or where documentation does not meet the standard, District Technology and the decision units will develop a plan to meet the standard.

**RATIONALE:**

Absent or out of date documentation means District Technology does not have the key programming documents it needs to support the software. For example, programmer analysts refer to documentation of programming routines in order to operate and maintain applications. Without this documentation, programmer analysts lose time gathering the information they need. In addition, software that has no documentation may pose a security risk to the district.

A coordinated approach is the most cost effective way to test new releases of district software. Consistent testing procedures allow decision units responsible for district applications to provide timely and accurate upgrade information to schools and central decision units. As well, an Integrated System Test plan reduces the risk of district software being compromised by the installation of new operating systems, network clients, office suites or upgrades to district software.

**PROCESS:**

Each DU is responsible for ensuring that proper documentation is maintained for all



applications for which they are responsible. In addition, these DU's must also ensure that the format and content of the documentation complies with district specifications.

Given these requirements, updates to documentation must be a component in the overall plan. District Technology will conduct periodic reviews to validate the content of the documentation, and will determine the evaluation criteria and the review frequency.

### **Guiding Principles for Testing**

#### *1. External Environment: (operating systems, network clients or office suites)*

- Major upgrades to software should not be installed without an Integrated System Test.
- New versions of software should not be adopted until three to six months after release. This allows vendors enough time to add necessary patches or 'fixes' to the original release.
- A new version of software will automatically trigger a review of specifications, such as 3A Computer Workstations for Staff, 3C Computer Workstations for Students and 4A MS Office Suite, regardless of the published review date.
- Where possible, schools and central services will receive advanced notice about any changes to the specification requirements so that they can plan effectively. They will be informed that a new version is expected and about the implementation process. A change impact assessment will be completed by District Technology as part of determining implementation timelines.

#### *2. Internal Environment: (upgrades to existing district applications or development of new district applications)*

- Major upgrades to software should not be installed without an Integrated System Test.
- Where possible, schools and central services will receive advanced notice about any changes to the specification requirements so that they can plan effectively. They will be informed that a new version is expected and about the implementation process. A change impact assessment will be completed by District Technology as part of determining implementation timelines.

### **Services and Support**

- District Technology is responsible for the costs of the test environment including hardware, software and related support.
- District Technology is responsible for the costs of setting up an Integrated System Test of district applications as a result of changes to the external environment. Decision units are responsible for providing staff to carry out the testing.

- All costs associated with an Integrated System Test resulting from updates or new developments initiated by a central services decision unit will be the responsibility of that decision unit.
- In addition to notices in the Superintendent's Memo, a new section will be added to the District Technology web site to provide information about upcoming changes and the direction the district is taking.

### **Test Environment**

- District Technology will set up and maintain a test environment on a continuous basis. The test server will house district applications typically used in our school environments.
- There are two drivers of change:
  - Internal Driver: A Central Services decision unit updates an existing software application or a new application is developed.
  - External Driver: New versions of operating systems, network clients or office suites are released.
- Both internal and external changes should initiate an Integrated System Test of all district applications housed on the test environment server.

---

**See also:** [Documentation Standards Template](#)