

SUBJECT: INFORMATION CLASSIFICATION

Supersedes: None; New policy
Effective: February 15, 2005
Page: 1 of 2

1.0 POLICY

Data classification and allocation of responsibilities for its ownership are important to ensure that the value of information is properly recognized. Employee responsibilities and the need to classify information are initially addressed in Detroit Public Schools (DPS) Information Security Policy 13.03. It is the first step towards ensuring that the most valuable information assets have the highest level of protection. Information varies in its degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling. DPS information classification process will be used to define an appropriate set of protection levels and communicate the handling measures.

Listed below are the business reasons for this process. They include, but are not limited to:

- Staying competitive (maintaining student enrollment)
- Ensure personal and group privacy – our employees
- Meet legal and regulatory requirements (Family Education Rights & Privacy Act - FERPA)
- Responsibility to our parents, students, and business partners
- Avoid adverse public Opinion
- Produce correct business decisions (accurate information that is available)

2.0 SCOPE

Information can be defined as ... any communication or information such as facts, data, or opinion, whether true or not, whether recorded in a material form or not, whether numerical, graphic or narrative, and whether maintained in any medium, including computerized databases, paper, microform, optical disk, or magnetic tape. DPS employees and business partners (contractors, vendors) have a responsibility to protect the security of, access to, correction of, use of, and disclosure of data.

3.0 ISSUANCE OF REGULATIONS/STANDARD OPERATING PROCEDURES

The Chief Technology and Information Systems Officer (CTIO) has developed regulations and/or standard operating procedures to implement this policy.

4.0 FAILURE TO COMPLY

Failure to comply with this policy and/or the corresponding regulations may result in a recommendation to the Chief Executive Officer for appropriate disciplinary action.

5.0 EXCEPTIONS

Any exceptions to this policy must be documented and approved by the DPS Chief Technology and Information Systems Officer. The DPS Technology and Information Systems Network Manager will monitor actions that will create exceptions.

6.0 AGREEMENT

I, _____ (print name) have read the Detroit Public Schools Information Classification policy, dated _____. I understand it and agree to abide by it. I agree to obtain prior approval if I should be required to perform a DPS business function that does not abide with the policy. If I should suspect a security breach in the disclosure, accuracy or availability of DPS informational assets, I will contact either my manager or the DPS Division of Technology and Information Systems. I further acknowledge that misuses of informational assets will result in appropriate disciplinary action.

Attachments: Administrative Regulation 13.04 – Information Classification

See also: Document Retention Schedule, Office of General Counsel 5/24/02

Legal References: Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99).

Labor Contract References: None

**DETROIT PUBLIC SCHOOLS
ADMINISTRATIVE REGULATION**

INFORMATION CLASSIFICATION

This Administrative Regulation implements Detroit Public Schools Policy 13.04 – Information Classification

1.0 Information Categories

DPS has developed four information categories that identify the level of protection that will be given

- Public - Non-sensitive information available for external release.
- Internal - Information that is generally available to employees and approved non-employees.
- Confidential - Information that is sensitive within the district and is intended for use only by specified groups of employees.
- Restricted - Information that is extremely sensitive and is intended for use only by named individuals within the district

2.0 Responsibilities

DPS information owners (as defined in Information Security Policy 13.03) are responsible for data classification based on the value and sensitivity of the information, for approving access, and communicating additional risk-based requirements. The data custodians are responsible for ensuring this policy is controlled and complied with. All employees (and this is taken to include anybody with access to data, including contractors, consultants etc) are responsible for ensuring they comply, by marking and treating all computer media and printed information with the appropriate classification and following established processes.

3.0 Information Categories and Access

	PUBLIC	INTERNAL	CONFIDENTIAL	RESTRICTED
Description	Non-sensitive information available for external release.	Information that is only sensitive outside the district. Generally available to employees and approved non-employees.	Information that is sensitive within the district, and is intended for business use only by specific groups of employees.	Information that is extremely sensitive, of highest value to the district and intended for use by named individual(s) only.
Examples	<ul style="list-style-type: none"> ▪ District advertising literature once issued ▪ District public announcements ▪ District activities 	<ul style="list-style-type: none"> • District business data • District organization charts • Internal announcements 	<ul style="list-style-type: none"> • Student identification information • Personnel (HR) information • Operating Plans • Technologies 	<ul style="list-style-type: none"> • Strategic plans • Business directions • Financial results prior to release • Operating procedures

	PUBLIC	INTERNAL	CONFIDENTIAL	RESTRICTED
Impact of: <ul style="list-style-type: none"> ▪ Unauthorized Disclosure ▪ Accuracy ▪ Availability 	No adverse impact	Limited adverse impact if disclosed 100% error free Part of Disaster Recovery Plan as non-critical	Significant adverse impact if disclosed: <ul style="list-style-type: none"> • May incur financial or legal liabilities • May adversely affect the district, its employees, its students or parents • Cause district embarrassment • May undermine confidence in the districts educational abilities 100% error free Critical data in Disaster Recovery Plan	Severe adverse impact if disclosed: <ul style="list-style-type: none"> • May cause severe financial or legal damage to the district • May prejudice the actual financial existence of the district, its employees, its students and its parents • May destroy confidence in the district • May damage the district's reputation 100% error free Critical data in Disaster Recovery Plan
Access Restrictions	Accessible to all employees and the community	Access normally restricted to employees and approved non-employees for business purposes only	<ul style="list-style-type: none"> • Access must only be granted on a business need to know • Access by external parties must be subject to a non-disclosure agreement as well as a business need to know 	<ul style="list-style-type: none"> • Access must be limited to named authorized individuals • Access lists must be maintained • Information must not be shown to or discussed with anyone not authorized • Access by external parties must be subject to a non-disclosure agreement as well as a business need to know

4.0 Storage, Labeling, and Disposal

	PUBLIC	INTERNAL	CONFIDENTIAL	RESTRICTED
Storage of Information (electronic)	No security control requirements	Site/Department storage should be adequate to prevent casual disclosure	Information may require encryption, where it does approved methods must be used.	Information must be encrypted using district-approved methods
Storage of Information Medium	No security control requirements	Site/Department storage should be adequate to prevent casual disclosure	Medium must be kept in locked storage or a secure environment (Notes 1 and 2)	<ul style="list-style-type: none"> • Medium must be kept in a locked drawer or equivalent, to which the addressee has sole access • Medium must be locked away when not physically in the presence of the originator or addressee (Note 3)
Labeling of Information (documents only)	Labeling not required	Labeling not required	Each page must be marked 'CONFIDENTIAL'	<ul style="list-style-type: none"> • Each page must be marked 'RESTRICTED' • Individual copies of the document must contain a unique identifier
Labeling of Information Medium (e.g. diskettes)	Labeling not required	Labeling not required	Where information medium is not permanently held in locked storage or a	<ul style="list-style-type: none"> • The information medium must be marked 'RESTRICTED' • Individual copies must

	PUBLIC	INTERNAL	CONFIDENTIAL	RESTRICTED
			secure environment, it must be labeled 'CONFIDENTIAL' (Note 4)	contain a unique identifier
Disposal of Information (electronic)	Removal of Directory entry for file Reference "Document Retention Schedule", Office of the General Counsel 5/24/2002	Removal of Directory entry for file Reference "Document Retention Schedule", Office of the General Counsel 5/24/2002	In addition to removing the directory entry for the file, the space used by the file must be over-written using data erasure procedures which adhere to Department of Defense (DoD) Standard 5220.2 for total erasure of confidential material Reference "Document Retention Schedule", Office of the General Counsel 5/24/2002	Network Drives: <ul style="list-style-type: none"> In addition to removing the directory entry for the file, the space used by the file must be over-written using data erasure procedures which adhere to DoD Standard 5220.2 for total erasure of confidential material Workstation or Laptop Drives: <ul style="list-style-type: none"> Physical destruction Reference "Document Retention Schedule", Office of the General Counsel 5/24/2002
Disposal of Physical Medium (e.g. paper/magnetic media)	Informal disposal Reference "Document Retention Schedule", Office of the General Counsel 5/24/2002	All media must be regarded as "confidential" information and be disposed of securely using methods approved by the Security Officer (i.e. shredding) Reference "Document Retention Schedule", Office of the General Counsel 5/24/2002	ALL media must be regarded as CONFIDENTIAL information and be disposed of securely using approved method (i.e. shredding) and based on retention strategies. Reference "Document Retention Schedule", Office of the General Counsel 5/24/2002	<ul style="list-style-type: none"> Information must be disposed of securely using approved methods (i.e. shredding) and based on retention strategies A record must be kept of how, when, and by whom the information was destroyed (To provide an audit trail) Reference "Document Retention Schedule", Office of the General Counsel 5/24/2002
<p>N.B. Medium means any physical item that contains information e.g. tape, diskette, paper document, CD</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. A secure environment is a physically secure area e.g. computer room, where written authorization is required in order to remove any information storage medium (e.g. tape). 2. If any member of staff finds a confidential item and it is not properly secured, it is their responsibility to secure it in accordance with the classification label attached to it. Immediately contact department leadership or the Division of the Chief Technology and Information Systems Officer 3. If any member of staff finds such an item that is not being actively used and is not stored securely, it is their responsibility to secure it in accordance with the classification label attached to it. Immediately contact department leadership of the Division of the Chief Technology and Information Systems Officer 4. Examples when labeling would be required are: a printed report containing Confidential information being circulated around a department or a PC diskette containing Confidential information that is used during the day and locked in a drawer outside working hours. 				

5.0 Distribution

	CONFIDENTIAL	RESTRICTED
Distribution	<ul style="list-style-type: none"> • Distribution lists of those groups authorized to receive information must be checked regularly to ensure currency • Distribution must be kept to a minimum • The item may only be copied or distributed by the originator of this item or the addressee • Items must be labeled with the classification before any copies may be made 	<ul style="list-style-type: none"> • Distribution is to named individual(s) only • The originator of the information item must keep a record of the unique identifier associated with the copy, and the named individual designated to receive that copy • The item may only be copied or distributed by the originator of the item • Items must be labeled with the classification before any copies are made
Addressing	<ul style="list-style-type: none"> • The storage medium must have two envelopes/layers of packaging • The outer envelope/layer must show the recipients name and address, be marked 'TO BE OPENED BY ADDRESSEE ONLY', and show the name and phone number of the sender of the information 	<ul style="list-style-type: none"> • The storage of medium must have two envelopes/layers of packaging • The outer envelope/layer must show the recipients name and address, be marked 'TO BE OPENED BY ADDRESSEE ONLY', and show the name and phone number of the Sender of the information
Dispatch of Information (except EDI)	<ul style="list-style-type: none"> • Packaging should ensure physical protection of the item. • Normal mail service 	<ul style="list-style-type: none"> • By hand or approved courier • Packaging must ensure physical protection of the item • Printed information sent through internal mail, external mail, or by courier must be sent by trusted courier or registered mail. The method of mailing must provide tracking.
Dispatch of Information (EDI)	Information may require encryption (if so approved methods must be used) when transferred via public networks (internet)	<ul style="list-style-type: none"> • Must be encrypted when transferred via public or private networks. (Note 1) • Electronic mail should use digital signatures for sending non-public information. • Information must not be faxed unless controls are taken to ensure proper control at the receiving end (password protected mailboxes, or person standing by to receive)
Voice	<ul style="list-style-type: none"> • Voice mail messages should be deleted as soon as possible (a written document from the sender is preferable). • Messages must not be forwarded (in case of misdialing or unauthorized access to other mailboxes). 	<ul style="list-style-type: none"> • Information must never be discussed on speaker-phones or during teleconferences unless all participating parties acknowledge first that no unauthorized persons are in close proximity, such that they might overhear the conversation • Information must never be discussed on cordless or cellular telephones
Note 1: Country-specific legal and regulatory requirements should be reviewed concerning the use of encryption technology.		