

## Working With Internal/Confidential Information

All district employees should use this document as a guideline to ensure the protection of sensitive information. For more information about the district’s Information Privacy and Security Program (IPSP) information classification scheme, please see:

<http://www.dcccd.edu/Employees/Policy+and+Procedures/IPSP/>

Information Types .....	2
Internal Information .....	2
Confidential Information .....	2
Securing Internal/Confidential Information .....	3
Sharing Information .....	3
Storing Information .....	3
E-mailing Information .....	3
Faxing Information .....	3
Viewing Information .....	4
Relating/Overhearing Information .....	4
Physically Securing Information .....	4
Disposal of Internal/Confidential Information .....	4
Securing Your Workstation .....	4
Securing Accounts and Passwords .....	4
Password Security .....	4
Use of Novell Login ID .....	5
Information Requests .....	5
Written Requests .....	5
Confidential Information Contacts .....	5
Location Information Privacy and Security Officer .....	5
Violations and Reporting .....	5
Violations .....	5
Reporting Security Breaches/Incidents/Issues .....	6
Terms .....	6
Related References .....	7

## *Information Types*

### **Internal Information**

This information is generally considered only for internal use by district school officials (see definition under Terms, below) as needed for their job functions and is not disclosable to the public unless required by law.

- Colleague ID (student/employee)
- Driver's license number
- Student directory information marked private:\*
  - Name
  - Home address
  - Home phone number(s)
  - E-mail address
  - Date and place of birth
  - Field of study
  - Classification
  - Enrollment status
  - Degrees and awards received
  - Dates of attendance
  - Participation in officially recognized activities and sports
  - Weight and height of members of athletic teams
  - Most recent previous school attended
  - Photographs

*\*Note: The above student directory information may be flagged as private at the request of the student and if flagged, must not be disclosed as public information. Contact your Registrar's Office for more information.*

- Employee information marked private:\*\*
  - Home address
  - Home phone number(s)
  - Any information that reveals family members of an employee

*\*\*Note: The above employee information may be flagged as private at the request of the employee and if flagged, must not be disclosed as public information. Contact Human Resources for more information.*

### **Confidential Information**

This information is private and requires protection with the highest levels of security, as prescribed by applicable laws, regulations and standards including, but not limited to, PCI Data Security Standard, GLB, FERPA, HIPAA, USA PATRIOT Act and Texas Administrative Code, Information Security Standards for Higher Education. This information is available to district school officials on a business need-to-know basis (based on applicable laws, regulations and standards).

- Social security numbers (SSNs)  
*SSNs are not generally needed to uniquely identify faculty, staff or students since all students and employees are assigned a unique Colleague employee/student ID. Unless SSNs are specifically needed, SSNs should be replaced with Colleague IDs in spreadsheets, reports, forms, non-Colleague databases, e-mails, etc. If the use of SSNs are specifically needed, they must be secured as confidential information.*
- Passwords (note: see password security section below)
- Credit or debit card numbers (and security codes) or bank account numbers
- Grades and academic standing
- Medical records protected by HIPAA

# ***Securing Internal/Confidential Information***

## **Sharing Information**

Never share internal or confidential information with any unauthorized person, within DCCCD or externally. (Note: An authorized person is one whose individual DCCCD account/password authorizes access; when in doubt, check with your supervisor.)

## **Storing Information**

Never store confidential information on any computer drive (e.g., C: drive) or external storage device (e.g., a USB or floppy disk drive, PDA, removable hard drive, etc.) without the explicit approval of your location Information and Privacy Security Officer (IPSO). Instead, store it on a secured DCCCD network drive (e.g., U:, P: drives, etc.) that limits access to authorized users only. If approval has been obtained from your location IPSO to store confidential information on a non-network DCCCD drive for official business purposes, it must be encrypted using an encryption method approved by your location IPSO, and viewing/accessibility must be restricted to only authorized people at all times.

## **E-mailing Information**

Never send (or solicit) confidential information via e-mail unless it is transmitted securely as specified below. Otherwise, it can be intercepted and is not secure.

- Internal e-mail from one DCCCD GroupWise e-mail address to another DCCCD GroupWise e-mail address: Currently, GroupWise is not a secure means of sending e-mail internally to other GroupWise recipients unless the confidential information is sent as an attachment that has been securely encrypted (see below). (Note: DCCCD is currently pursuing the means to allow confidential information to be sent via GroupWise e-mail within DCCCD.)
- E-mail from a DCCCD GroupWise e-mail address to any external e-mail address: When sending confidential information, it must be sent as an attachment that has been securely encrypted (see below).
- Securing e-mail attachments: Confidential information sent as an attachment must be encrypted using an encryption method approved by your location IPSO.
- Instant messenger (IM): Never send confidential information via instant messenger.

## **Faxing Information**

If it is necessary to fax internal or confidential information, appropriate precautions must be taken: Exception: Credit card account numbers must not be solicited or accepted via fax.

- Use a cover sheet indicating “Internal/Confidential Information Enclosed”; it should also include the date and time, sender’s name, authorized recipient’s name, number of pages transmitted and information regarding verification of receipt.
- A warning should be placed on the bottom of the fax cover sheet: “Important Warning: This message is intended for the use of the person or entity to which it is addressed and may contain information that is privileged and confidential, the disclosure of which is governed by applicable law. If the reader of this message is not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this information is strictly prohibited. If you have received this message by error, please notify us immediately and destroy related message.”
- Limit the faxing of internal/confidential information to urgent or non-routine situations when mail or other delivery is not feasible.

- Call ahead to alert the receiver so that they can promptly retrieve the information.
- Regularly empty the fax tray so internal/confidential information does not remain exposed on the fax machine for long periods of time.
- Confirm the accuracy of fax numbers. All commonly used fax numbers should be programmed into the fax machine to prevent misdialed numbers.

## **Viewing Information**

- Never allow internal or confidential information to be viewable/accessible in any format or on any device at work, home or any public/private place if doing so would allow it to be viewable/accessible by any unauthorized person. (Note: An authorized person is one whose individual DCCCD account/password authorizes access based on a business need-to-know; when in doubt, check with your supervisor.)
- Positioning of monitors, use of privacy screens, etc., should be used when necessary to prevent the unauthorized viewing of confidential information in publicly accessible areas.

## **Relating/Overhearing Information**

Never allow confidential information (especially credit card numbers or SSNs) to be overheard by unauthorized people (e.g., by repeating confidential information aloud, during conversations, using a speakerphone, etc.).

## **Physically Securing Information**

Keep rooms and file cabinets where confidential information is kept (especially workspaces in public areas) locked in order to restrict access to only authorized people.

## **Disposal of Internal/Confidential Information**

Properly dispose of any internal (if used in combination with other personally identifiable information) or confidential documents and media that are no longer required/needed (e.g., papers, files, CDs, floppy disks). For more information concerning the retention, storage and disposal of information, contact the District Service Center (DSC) Records Management Department.

## **Securing Your Workstation**

- Use the Windows/Novell “Lock Workstation” feature to lock your workstation whenever you leave your workstation unattended. (Note: You can lock your workstation by using the following Windows shortcut: Simultaneously press the Windows logo + L keys. (The Windows logo key on your keyboard is the one that looks like the Windows logo, or a flag; the letter L can be either upper or lowercase.) Use your Novell password to unlock your workstation.
- Workstations in areas open to the public should set up a password protected screensaver that automatically comes on within at least 30 minutes of inactivity.

## ***Securing Accounts and Passwords***

### **Password Security**

- Use strong passwords (i.e., at least eight (8) characters in length with a combination of letters and numbers). See the document “How to Create Strong Passwords” for further details on this subject.
- Use passwords that you can remember so you won’t have to write them down.

- Change passwords periodically.
- Change your password immediately if you think anyone else knows your password.
- Do not give your password to anyone. (Note: Only in rare situations will an IT staff member need to know your password to fix a reported problem. After the problem has been resolved, you must change your password so that only you know it.)
- Do not reuse DCCCD work-related passwords for access to systems, accounts or services outside of the DCCCD environment.
- Do not use any feature (e.g., “remember my password”) that remembers your password for logging in to applications/systems containing confidential information.

## **Use of Novell Login ID**

Never use your Novell login ID for external use in the form of an external account name, login or e-mail address. For example, never use your formatted GroupWise e-mail address (e.g., [ABC1234@dcccd.edu](mailto:ABC1234@dcccd.edu)) with non-DCCCD contacts, on business cards, on Web sites, as a GroupWise e-mail signature or in any print publications, documents, etc.; only use your GroupWise e-mail address *alias* (e.g., the alias used in the DCCCD public staff directory at: <http://www.dcccd.edu/About+DCCCD/Contact+Us/Staff+Directory.htm>).

## ***Information Requests***

### **Written Requests**

For written requests received for student directory information, notify and send to the Registrar’s Office. For all other written requests, fax to District Legal.

### **Confidential Information Contacts**

- FERPA regulations: location Registrar’s Office
- Gramm-Leach-Bliley (GLB) Act or handling of credit card and financial information: location Business Office
- Handling of employee information: location Human Resources Department
- Handling of HIPAA (health or medical) information: location Health Center
- Retention, storage and disposal of information: DSC Records Management Department

### **Location Information Privacy and Security Officer**

Contact information for your location Information Privacy and Security Officer (IPSO) can be found by following the link from the DCCCD Information Privacy and Security Program Web site at: <http://www.dcccd.edu/Employees/Policy+and+Procedures/IPSP/> or on the DCCCD intranet at: <http://dsc3.dcccd.edu/intranet/dcccd/infosecurityprogram/IPSPCommittee/IPSOOfficers.htm>

## ***Violations and Reporting***

### **Violations**

In accordance with Board Policy DH (LOCAL), VIOLATIONS: “Employees shall comply with the standards of conduct set out in this [DH (LOCAL)] policy and with any other policies, regulations, and guidelines that impose duties, requirements, or standards attendant to their status as District employees. Violation of any policies, regulations, and guidelines may result in disciplinary action, including termination of employment.”

[http://www.tasb.org/policy/pol/private/057501/pol.cfm?DisplayPage=DH\(LOCAL\).html](http://www.tasb.org/policy/pol/private/057501/pol.cfm?DisplayPage=DH(LOCAL).html)

## Reporting Security Breaches/Incidents/Issues

Immediately report any situation that affects the confidentiality, integrity and/or availability of confidential information to your location's IPSP incident response coordinator. For more information, see "Information Privacy & Security: Reporting an Information Breach" at: <http://www.dcccd.edu/Employees/Policy+and+Procedures/IPSP/>

## *Terms*

**authorized person:** An authorized person is one whose individual DCCCD account/password authorizes access based on a business need-to-know; when in doubt, check with your supervisor.

**confidential information:** This information is private and requires protection with the highest levels of security, as prescribed by applicable laws, regulations and standards including, but not limited to, PCI Data Security Standard, GLB, FERPA, HIPAA, USA PATRIOT Act and Texas Administrative Code, Information Security Standards for Higher Education. This information is available to district school officials on a business need-to-know basis (based on applicable laws, regulations and standards).

**event:** An observable occurrence; an aspect of an investigation that can be documented, verified and analyzed.

**FERPA:** Family Educational Rights and Privacy Act

**GLB:** Gramm-Leach Bliley

**HIPAA:** Health Insurance Portability and Accountability Act

**incident:** An adverse event or series of events that impact the privacy/security of the district, its customers, its public image and/or the ability of the district to do business.

**information classification scheme:** The classification level given to information – according to its use, sensitivity and importance – that determines how information is to be handled and protected within DCCCD. The three categories of information are as follows:

- Category I – Public Information
- Category II – Internal Information
- Category III – Confidential Information

**internal information:** This information is generally considered only for internal use by district school officials as needed for their job functions and is not disclosable to the public unless required by law.

**IPSO:** information privacy and security officer

**IPSP:** Information Privacy and Security Program

**location IPSP incident response coordinator:** The vice president-level location employee and/or their designee responsible for coordinating the location's response (in conjunction with the district IPS incident response coordinator) to a privacy/security event or incident.

**PCI:** payment card industry

**personally identifiable information:** Information that alone or in conjunction with other information identifies an individual.

**school officials:** Any employees, trustees or agents of the district, as well as attorneys, consultants and independent contractors who are retained by the district. School officials have a "legitimate educational interest" in a student's record when they are working with the student; considering disciplinary or academic actions or the student's case; compiling statistical data; or investigating or evaluating programs.

**USA PATRIOT Act:** Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism

## ***Related References***

- **Board Policies**
  - CS(LOCAL) Information Security  
[http://www.tasb.org/policy/pol/private/057501/pol.cfm?DisplayPage=CS\(LOCAL\).html&QueryText=CS](http://www.tasb.org/policy/pol/private/057501/pol.cfm?DisplayPage=CS(LOCAL).html&QueryText=CS)
  - CS(REGULATION) Information Security  
(URL TBA)
  - Violations DH(LOCAL) Employee Standards of Conduct  
[http://www.tasb.org/policy/pol/private/057501/pol.cfm?DisplayPage=DH\(LOCAL\).html&QueryText=DH%20LOCAL](http://www.tasb.org/policy/pol/private/057501/pol.cfm?DisplayPage=DH(LOCAL).html&QueryText=DH%20LOCAL)
- **District Information Privacy and Security Program (IPSP) Web site**  
<http://www.dcccd.edu/Employees/Policy+and+Procedures/IPSP/>
- **How to Create Strong Passwords**  
<http://www.dcccd.edu/Employees/Policy+and+Procedures/IPSP/Passwords/>
- **Information Classification Scheme**  
<http://www.dcccd.edu/Employees/Policy+and+Procedures/IPSP/>
- **Texas State Law**  
[http://www.tlc.state.tx.us/legal/b&c/code/b&c\\_title11/80C359\(3\).html](http://www.tlc.state.tx.us/legal/b&c/code/b&c_title11/80C359(3).html)