



Data Director

Acceptable Use Policy

(Version 1.4)

What is Data Director?

Data Director is a web-based data warehousing system developed by Achieve Data Solutions. It contains data from several Santa Monica-Malibu Unified School District (SMMUSD) databases all collected together in one place. For example, the Student Information System (SIS) data and the California CAHSEE and STAR assessment data are copied into Data Director. This allows aggregated and disaggregated reports to be built using Data Director. There are regular extracts of SIS and assessment data into Data Director meaning that Data Director is always populated with the most current information available.

What is an acceptable use policy?

An acceptable use policy is meant to cover issues of computer and data use—what is permissible and what is not. The scope of this acceptable use policy is limited to Data Director. The policy is issued to all users of the Data Director system and the user's signature is required before a login to Data Director will be issued. This helps to communicate the district's expectations of data use and the user's understanding and acceptance of these expectations.

Information security

One of the most valuable assets of SMMUSD is its information. Local, state, and federal laws require that certain types of information (e.g., individual student records) be protected from unauthorized release. This facet of information security is often referred to as protecting confidentiality. While confidentiality is sometimes mandated by law, common sense and good practice suggest that even non-confidential information in a system should be protected as well. Parents and students expect that student record confidentiality will be maintained at all times and it the district's expectation that all Data Director users will treat confidentiality as their highest priority.

- What SMMUSD Information Services will do
 - Maintain the Data Director software with Achieve Data Solutions.
 - Secure the physical Data Director server.
 - Manage and protect the Data Director user accounts and login process.
 - Provide daily backups of Data Director.
 - Provide near 24x7 availability to Data Director.
 - Record every login by every Data Director user.

- What SMMUSD Data Director users will do
 - E-mail – Use SMMUSD e-mail only for routine office communication. Sending student records or sensitive information in an e-mail puts the student's confidentiality at risk since the e-mail could be forwarded to someone not authorized to view confidential student records.
 - Viewing student records – It is extremely easy to display student records on a computer screen in Data Director. Confidential information is readily available. This information is for the consumption of the logged in Data Director user only. **Do not** leave the computer screen unattended without locking it first.

- Storing student records – Downloading student records from Data Director into files is permissible but storing them **must** be protected. Data Director permits almost all student data to be downloaded into Excel files and other kinds of files. It's the Data Director user's responsibility to protect the student confidentiality contained in these files.
- Printing student records – Printing confidential student information is very convenient in Data Director. However, any printed material is confidential. Printed student records **may not** be disposed of in regular trash containers. They should be shredded to protect confidentiality. All addresses, phone numbers and any other student demographics are confidential and **may not** be shared with non-SMMUSD staff, even parents.
- A note on sharing student records in Data Director
 - Student records are generally visible on a need-to-know basis.
 - It is not breaking confidentiality to share student records among people who have access to the same group of students (e.g. teachers can share student records with their principal or other collaborative SMMUSD staff working with the student).
 - Student records **may not** be shared with non-SMMUSD staff.
 - It may be permissible to share some student information with SMMUSD staff when student names and identifiers have been removed.
 - Some Data Director reports allow for aggregation by subgroup (e.g. African-American, Hispanic, etc.). When the number of student records in the aggregated report value is less than 10 per grade level, state law prevents SMMUSD staff from releasing the report since the students may be easily identifiable even without their names listed on the report.
 - Parents or legal guardians may only see student records related to their students.

User access security

User access security refers to the collective procedures by which authorized Data Director users access the system and unauthorized users are kept from doing so. User access security limits are also a part of this policy. For example, site administrators are only able to access records for students at their site. Teachers are able to only access their current students.

- All Data Director users should expect the following
 - To sign, date and complete the Data Director Acceptable Use Policy (this document)
 - Upon successfully logging into Data Director the first time, a new password must be set.
 - Passwords **must** be a minimum of six characters/numbers/symbols.
 - A user name **cannot** be used as a password.
 - Periodic password changes will be required.
 - User names and/or passwords **may not be shared**, sent in an e-mail or posted in any way.
 - If a computer has accessed Data Director in a public place (e.g. lab or classroom) it **cannot** be left unattended without first locking the screen or logging off.

I acknowledge that Data Director's information and technology security policies, guidelines, and procedures have been made available to me for adequate review and consideration. I also certify that I have been given ample opportunity to have any and all questions about my responsibilities addressed. I am, therefore, aware that I am accountable for information and technology security procedures as they govern the acceptable performance of my job. I understand that failure to abide by any and all Data Director policies, guidelines, and procedures can result in organizational, civil, or criminal action and/or the termination of my employment.

Signature: _____ Printed Name: _____

Site: _____ Job Title: _____ Date: ____/____/____

For further reading... Email: _____

Family Educational Rights and Privacy Act of 1974 (FERPA) fact sheet

<http://nces.ed.gov/pubs98/safetech/appendix-b.asp>

References

<http://nces.ed.gov/pubs98/safetech/index.asp>