

## Welligent Security Policy

1. The information housed by the Welligent System is protected by legislation. The access provided by each user account is accessible only by the individual assigned to that user account. Providing access to another user by sharing the name and password is strictly prohibited.

The end user must log into the system and out of the system according to the intended login and logout mechanism.

2. Information downloaded from the system is legally protected, and is only to be shared with other employees who normally have access to that information. Sensitive information should be treated with care once it is transferred to a local computer. It should not be shared by non-secure mechanisms, particularly email.

3. All End Users are responsible for following the District's Acceptable Use Policy in its entirety when accessing the system. This policy may be reviewed at:  
[http://techsupport.lausd.net/lausd\\_applications.htm](http://techsupport.lausd.net/lausd_applications.htm).

4. If an end user is suspicious that an intentional or unintentional release of confidential information has occurred, they are to notify the Planning, Assessment and Research Division IEP Support Section or ITD Welligent STS Support at the help line numbers.

5. Passwords should be chosen that are not based upon the user name, or common words found in the dictionary. Welligent password construction rules require at least 8 characters, including letters and at least two numbers, and cannot contain the user name. Passwords should not be written down if it is avoidable.