

BOARD CHAIR
Georgia "Joy" Bowen

BOARD VICE-CHAIR
Daryl Jones



BOARD MEMBERS
DeeDee Rasmussen
Alva Striplin
Rosanne Wood

INTERNET ACCESS AND SECURITY USER-ID AGREEMENT

I hereby acknowledge acceptance of a security user-id code, which allows me access to personally identifiable student, financial, or personnel information as appropriate to my assigned area of responsibility. I understand that much of this information is confidential under federal law, state law and the Policies of the School Board of Leon County, Florida. **I UNDERSTAND THAT:**

- I must only access that information in which I have direct and legitimate educational interest.
- I am personally responsible for taking reasonable steps to secure confidential data and to control distribution of confidential information.
- I understand that internet access is designed solely for education purposes and that I must use these resources only for educational purposes consistent with the educational mission and policies of Leon County School District.

I agree to follow all procedures designed to protect the confidentiality of personally identifiable student information, financial information and/or personnel information. I hereby acknowledge that I have read and agree to all procedures listed on School Board Administrative Procedure 7530A-Security of User Access to District Technology Resources and Administrative Procedure 7540.09-Computer Operating and Security Guidelines (Technology and Computer Use Manual).

I agree to be responsible for use of the district computer equipment. I agree to not leave computer equipment unattended while I am signed on to the District's Network. I agree to protect all data files and computer programs, by logging off the network, or locking my assigned equipment/office while unattended.

I agree to abide by all rules stated in the Administrative Procedures regarding disclosure of passwords. I understand that my failure to abide by these conditions shall subject me to formal disciplinary action.

I UNDERSTAND AND AGREE TO THE CONDITIONS SET FORTH IN THIS DOCUMENT.

Full Legal Name

Date of Birth (MM-DD only)

Last 4 SSN

Signature

Date

Technology and Information Services
520 South Appleyard Drive Tallahassee, Florida 32304-2998 Phone (850) 487-7530

Building the Future Together

"The Leon County School District does not discriminate against any person on the basis of sex (including transgender status, gender nonconforming, and gender identity), marital status, sexual orientation, race, religion, ethnicity, national origin, age, color, pregnancy, disability, or genetic information."

Leon County Schools: Technology and Computer Use

1. Activities must support education and school operations consistent with the educational goals and policies of the Leon County School District. The use of the internet and automated systems is not a right, but a privilege, and inappropriate use will result in cancellation of that privilege. School administrators will decide what is inappropriate use based upon guidelines, standards, policies and prudent judgment. User accounts shall be assigned or closed at the direction of the site or program administrator. It is the site administrator's responsibility to have a signed access use form on file for all users at that site prior to access authorization.

2. The person in whose name an account is issued is responsible for its proper use.

Unacceptable uses of the network include:

- Violating student or staff rights to privacy
- Using profane, obscene or offensive language, graphics or other forms of communication
- Use of school system technology resources in support of private or personal businesses; (business partners or interagency agreement agencies may be an exception)
- Misuse or sharing of passwords
- Reporting personal communications, email or faxes, or using personally identifiable information or individually owned or copyrighted material (this includes pictures, artwork, and products) without the author's (or parent's/guardian's) prior consent;

3. Persons using Leon County Schools internet or automated systems connections must be properly authorized. Users must have completed the necessary district authorization forms and agreements and these must be maintained on file at the school or department site. Access request forms are also kept on file at the Technology & Information Services Department. Automated systems access requires the site administrator's or program administrator's authorization and signature. Appropriate training on the respective system(s) is required prior to enabling system access. Students will not be granted access to Student and Business system applications. For students or staff (employees) under 18 years of age, a parent's signature is required for internet or automated systems use.

4. Any breach in security where confidential records may have been accessed or secure information altered is a very serious problem and must be reported to the school or department administrator and to the Technology & Information Services Department and to the Site Tech Contact immediately. This is necessary to secure systems which may be at risk and to track access records to resolve any access or data change problem. The site or program administrator will be notified of suspected access or distribution violations. It will be the responsibility of the respective administrator to follow up in investigating such reports and taking appropriate action, which may include criminal litigation.

5. Use of another individual's account (password) is a security violation. Attempts to log on as another user will result in cancellation of privileges and notification of the responsible administrators. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to all or part of the network.

6. Each employee working with or having access to confidential records should be informed and acknowledge that most personally identifiable information is confidential (and, often times, directory information as well). Only those persons having direct and legitimate interest in that student may view, access, or otherwise make use of such information. Those properly authorized persons are responsible for appropriate access, distribution, records security and destruction of confidential information whether "hard copy" (e.g., paper) or electronic.

Off-site internet and automated systems users should follow the same guidelines.