Fayette County Public Schools

Operational Guidelines [IFBG: Acceptable Use Policy]

Owner: Jim Farmer, Chief Technology Officer
Last Updated: February 26, 2024

Purpose

Fayette County Board of Education values the trust that parents place in our district to protect their personal and student data. As such, these operational guidelines provide individuals additional details on the security and protection of our systems and data. The purpose of the Responsible Use Policy is to protect staff, students, and stakeholders from potentially damaging actions. Examples in these guidelines are illustrative and not exhaustive.

The protection of Information security and data privacy is the responsibility of all individuals who interact with District information.

Definitions

- District: Fayette County Board of Education (FCBOE)
- Systems: Any District-owned or managed servers, cloud infrastructure, cloud applications, software, computers, laptops, mobile or other technology devices.
- Network: Any wired, wireless, or cloud-based networks available at District offices or remotely
- Individuals: Any person possessing or accessing District-owned devices or systems
- Employees: Any employee, including temporary, substitute, and contractors possessing or accessing District-owned devices or systems
- Students: Any enrolled or withdrawn student possessing or accessing District-owned devices or systems
- Confidential: Data that is considered confidential or higher as identified in Data Classification and Handling Guidelines.

Applicability

These guidelines apply to all Fayette County Board of Education employees, temporary and contract workers, students, and individuals who access District systems (technology based resources) and data.

Guidelines

1. Policy and Training Delivery

    1.1. Employees are required to annually complete the cybersecurity and privacy awareness courses designated by the District and sign an attestation confirming that the Responsible Use Policy has been read and understood through the required annual HR training documents.

    1.2. The District shall educate students about appropriate online behavior, including interacting with other individuals on social networking websites, chat rooms and other social platforms. Student attestation shall be performed through the Student Code of Conduct.

2. Use of District Systems and Devices

    2.1. District systems are to be used for District activities. Personal use should be limited.

2.2. District devices that are issued to individuals are the responsibility of that individual. Devices that are damaged under normal wear and tear will be replaced at no cost. Devices that are otherwise damaged will be replaced or repaired at the contract rate of an approved vendor and the individual may be required to cover some or all of the expense.

2.3. District devices should be secured when left unattended. It is the responsibility of the individual to protect District devices and data in their care. If a device is lost or stolen, the event should be reported immediately to Technology Services and appropriate law enforcement.

2.4. Vandalism of District property is prohibited and may result in disciplinary action. This includes any activity intended to harm or destroy District hardware, software or data, such as creating a computer virus, service disruptions, and physical damage. Abuse of a District device or system may also be subject to disciplinary action, and if applicable, legal actions.

2.5. District devices that are issued to individuals should be returned to the District immediately upon withdrawal (students) or termination of employment (employees and contractors).

3. Limited Personal Use

3.1. Limited personal use of District systems may be permitted except for the following conditions:

- Personal use shall not interfere with job duties, responsibilities, or performance. For employees compensated on an hourly rate basis, the use does not result in the District paying the employee wages for time spent on that personal use.
- Personal use shall be kept to a minimum and not incur any cost to the District, including the cost of paper or ink. Individuals utilizing District devices or systems in a manner that is not for District-related business will be required to pay all costs incurred.
- Personal use shall not involve data usage, app usage, or text messaging from any District-owned device where the usage results in a payment that will be charged to the District as the account holder.
- District employees are not permitted to use District-provided cloud storage for personal data. Cloud storage is to be used solely for District business purposes.
- Personal use shall not interfere with other individuals who are using District systems for appropriate business reasons or disrupt the intended use of District systems.
- Personal use shall not constitute any form of employment or business activity other than for the District.
- Personal use shall not include access to gambling, pornographic, or other inappropriate sites or materials.
- Personal use shall not include political campaigning or unauthorized fund raising.
- Personal use should not expose the District to unnecessary risks or violate applicable laws or other District policies.

3.2. Individuals must adhere to the above restrictions whether in the office, offsite, or accessing systems remotely.

3.3. Individuals must not install or use any software or application not approved by the District, including personally owned software and applications.

3.4. Personal Devices (devices not issued by FCBOE) are prohibited from connecting to the authenticated district network, either by physical connection or wireless access point. A guest network has been provided for any personal use devices and is the only approved method for devices not issued by the district to utilize the Fayette County Board of Education network for personal Internet access. Access from the guest network will not be provided to district private network resources.

3.5. Individuals shall immediately report lost computing devices, communications devices, phones, identification badges, or other devices used for identification and authentication purposes.

3.6. Individuals shall not engage in activities that could compromise the security of the District infrastructure. Password sharing, guessing or cracking, vulnerability scanning, disruption of network services, or other hacking activities are not permitted. It is the responsibility of each member of the faculty, staff and student body to report any unauthorized access or potential security compromise.

3.7. Individuals are expressly prohibited from deleting or tampering with electronically stored information. In the absence of an investigation, litigation, or legal hold, information may be deleted, destroyed, or disposed of upon the termination of the applicable mandatory retention period.

3.8. Information transmitted or received over a District-owned device or system should not be considered “private,” including the “Guest” network. Local, state or federal officials may obtain access to records of calls or texts placed via District-issued devices and systems in connection with investigations or other purposes. These records may also be subject to disclosure under the Georgia Open Records Act (§ 50-18-70).

4. Email, instant messaging, and text messaging

4.1. Individuals must use their District email account to communicate business matters on behalf of the District through email.

4.2. Individuals shall not use public email systems such as Yahoo mail, Gmail, etc. to communicate District business matters.

4.3. The District prohibits the use of District systems for unsolicited mass emails or commercial purposes unless preapproved by the District.

4.4. Individuals must not forward confidential business messages or other electronically stored information from their District accounts to a personal account, except for messages related to their personal benefits (e.g., retirement, health, and taxes) information.

4.5. Individuals must not use their District email address to register or create accounts on external websites (e.g., Amazon, eBay, etc.) for personal use except as required by official District-supported initiatives (e.g. District-sponsored social media accounts).

4.6. Individuals must not use District systems to create, store, send, or display pornographic, defamatory, spam emails, maliciously false material or the like. This applies regardless of whether any other individual is offended by or is even aware of the material.

4.7. Individuals are responsible for ensuring the proper use of their District email account. Any actions performed with an individual’s account is the responsibility of the email account holder.

4.8. Individuals should use extreme caution when opening email attachments or clicking on hyperlinks even when received from a known sender. Attachments and hyperlinks may contain malware and suspicious emails should be reported using the “Phish Alert” button in email.

4.9. Individuals are prohibited from conducting confidential District business via personal messaging or other means of written communication that are not managed by the District. This includes, but is not limited to, social media and personal email.

4.10. If an individual receives a confidential message related to District business via personal text messaging or personal email, that individual should inform the sender of this policy and request future communications be sent via approved methods (i.e. the individual's District email or phone number).

5. Copyright Information

5.1. Individuals should assume that any material accessed on District-managed systems is the property of another and that the use of the material is restricted by copyright laws unless there is definitive evidence to the contrary.

5.2. Individuals must comply with applicable copyright laws and terms and conditions of license agreements for software and published materials. In addition, individuals must ensure that software can be used without conflicting with any other policy.

5.3. Individuals must not use District systems to download, store, duplicate, distribute, print, or use copyrighted material from any source (e.g. published works or the Internet) without the copyright owner's permission.

5.4. The District accepts no responsibility for violation of copyright laws by employees, students, or other individuals.

6. Personally Identifiable Information

6.1. Individuals with access to personally identifiable student records shall adhere to standards included in the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C.§ 1232g and other applicable laws and regulations, as they relate to the protection of student education records.

6.2. Individuals shall not use access to student or employee records information for personal reasons. In no case shall personally identifiable information be released publicly.

6.3. Individuals shall refrain from viewing or printing personally identifiable information except to perform their assigned duties.

6.4. The "casual viewing" of student or employee data constitutes misuse of access is not acceptable.

6.5. District employees and contractors shall not be granted access to sensitive information that is not authorized based on job-related "need to know" or for a job-related "legitimate educational interest."

- ■ Sensitive information includes, but is not limited to:
  - Student or parent names, address, telephone numbers
  - Student ID, grade, attendance, medical, or transcript information
  - Student or parent financial or financial aid information
  - Social security number or GTID
  - Race/Ethnicity, date of birth, age
  - Employee name, address, telephone number
  - Employee payroll or benefits information
  - Any information which by itself or combined with other information would allow a person to be able to identify an individual

- Handling of PII or FERPA protected information

  - When transmitting PII or FERPA protected information via electronic media, District employees shall take appropriate precautionary measures to protect the confidentiality of the data. Communications may be subject to disclosure under the Open Records Act. Therefore, transmission of confidential information should be avoided.

  - When storing PII or FERPA protected information, portable storage media such as smartphones, USB drives, CD/DVDs, flash drives, and other portable devices are at risk of loss or theft of District data and must be protected at all times. Any employee who is authorized to store district data on portable media must utilize approved data protection encryption standards with a protected password.

  - Storage of sensitive data on network drives and cloud storage must be available only in a secured, password protected, and/or encrypted file.

  - All printed material containing sensitive information must be secured in a locked area when not in use. If the information is discarded, it must be shredded.

  - Sharing data, screenshots, files, etc. that contain sensitive information should only include information that is applicable to the person receiving the data in a “need to know” or “legitimate educational interest” as approved by the appropriate Business Process Owner of that data. Any data not needed should be removed, obscured, or redacted from the data being shared.

  - Unauthorized disclosure of protected information may result in civil or criminal penalties pursuant to any and all applicable State and Federal laws and/or removal of access to protected information, reassignment or removal of duties, and, in the case of a District employee, disciplinary action, up to and including termination.

6.6. Individuals authorized to access personally identifiable information shall execute a separate acknowledgement indicating they are aware of additional provisions of applicable laws and regulations. For employees, this shall be provided through the annual acknowledgement process provisioned through the Human Resources department.

7. File Sharing and Data Storage

7.1. The District uses predefined file sharing or storage services for communicating District business matters. Any non-standard service must be approved by Technology Services before use.

7.2. Individuals are responsible for making sure pertinent data is stored on District provided cloud or network storage locations to ensure data is backed up in a manner that the data can be restored in the case of theft, loss, or system crash. Data stored on individual devices are not backed up.

7.3. Individuals shall not use non-approved online storage solutions to store District data (e.g. Dropbox, OneDrive, Mega, etc.). Only District-provided storage resources should be used to store data.

8. Internet and Network Usage

8.1. Only District-approved devices are permitted to connect to the District network while on-premise at District facilities.

8.2. A guest network is provided for individuals, such as visitors, vendors, parent liaisons, volunteers, etc., to which non-District-owned devices can connect to gain access to the Internet.

8.3. The District prohibits the use of District resources and network access by non-employees unless pre-approved by Technology Services.

8.4. Employees should not connect District systems to the guest network while on-premises at District facilities.

8.5. Individuals must not attach devices to the District's network that provide wireless access or other shared network connections to the District network (such as wireless routers or cell phones used as wireless hotspots).

8.6. Individuals are not allowed to host personal websites on District systems including sites hosted on the Google Workspace for Education domain.

8.7. The District reserves the right to block access to Internet sites deemed inappropriate (e.g., sexually explicit, gambling-related sites), lacking educational or work-related content, or those that pose a threat to the network.

8.8. Individuals are not allowed to produce personal web pages or websites that appear to be official District or school webpages or websites.

8.9. Individuals shall not run their District laptops or district issued phones and devices in wireless sharing or hot spot modes. This potentially allows other users to connect to the device in a peer-to-peer connection.

8.10. Individuals shall not utilize any remote access software, tools, or technologies, including but not limited to, Windows Remote Desktop (or other third-party remote applications), unless specifically approved by District Technology Services.

9. Protecting Access to District Systems

9.1. The District reserves the right to remotely manage and enforce security policies on all devices that connect to the District systems and wipe any District-specific data on the devices at its discretion.

9.2. Individuals must take appropriate actions to protect from loss or theft District-owned devices and non-District-owned devices that have been approved to access District systems.

9.3. Individuals should always lock their screens when leaving devices with access to District-systems unattended.

9.4. Individuals must not permit anyone who is not authorized (e.g., family member or friend) to use a District-owned device or application (even if on a personal device) to access District systems for any purpose.

9.5. Individuals must cooperate with Technology Services-related activities such as helping to resolve security incidents.

9.6. Individuals shall not share District accounts, personal identification numbers, identification badges, or other devices used for identification and authentication purposes.

9.7. Individuals must promptly report the theft, loss, or unauthorized disclosure of District information and assets, including employee badges, crisis alert badges and District-provided encrypted key fobs.

9.8. Individuals shall immediately report any suspected account compromise, data breach, or suspected cybersecurity incident by calling Technology Services at 770-460-3535 ext. 6018 as well as reporting to a direct supervisor.

9.9. Access to District systems and information is provisioned based on an employee’s job responsibilities. All access shall be requested and monitored by the individual’s supervisor.

9.10. Individuals should not access District data they are not expressly authorized to access.

9.11. Individuals should immediately report if they discover they are able to access data they are not authorized to access. Employees should report in writing to a supervisor; students may report to any District staff member.

10. Password Management and Authorization

10.1. Individuals must keep passwords private, securely hidden, and protected and must not share passwords with anyone unless they are authorized and authenticated for such access. This includes managers, support staff members, or Technology Services personnel.

10.2. Individuals should create passwords that, at a minimum, adhere to the recommended character length and complexity guidelines set forth by Technology Services.

10.3. Individuals may use password storage technology on District-owned devices if that technology uses multi-factor authentication (MFA) such as biometric, SMS, or authenticator-based MFA.

10.4. Individuals may not circumvent any authentication or security mechanism, nor modify, bypass, or disable the security configuration of any District-owned device.

10.5. Individuals should immediately notify an administrator and Technology Services if their password is lost or stolen or if they believe someone has obtained unauthorized access to an account password.

11. Review and Monitoring the Use of District Systems

11.1. Except for any privilege or confidentiality recognized by law, individuals have no legitimate expectation of privacy in the use of technology resources. The district reserves the right to monitor, intercept, access, copy, and disclose the contents of any user's files, activities, or communications without prior notice to the individual.

12. Leaving the District

12.1. Upon termination or withdrawal from the District, individuals must return all District-owned devices, property, equipment, and electronically-stored information to the District through the school or department in which the individual is assigned or enrolled.

13. Violations

13.1. Any individual who violates the Responsible Use Policy or its guidelines are subject to disciplinary action, and if applicable, legal actions. Violations of this policy will be evaluated on a case-by-case basis and the level of discipline imposed shall be based on the seriousness of the offense.

13.2. Employee disciplinary actions may be up to and include termination.

CoSN: NIST Cybersecurity Framework Resources for K-12

Reference: IFBG: Internet Acceptable Use Policy