Governor's Education Emergency Relief

Considerations for Use of Personal Smartphones by Staff

When teachers use personal phones to gather student data including photos, there are potential risks regarding privacy and data protection, particularly under laws like the **Freedom of Information Act (FOIA)**. Here's an explanation of how the FOIA can impact a teacher's use of a personal smartphone to gather and store student data:

Understanding FOIA and Its Impact

The **Freedom of Information Act (FOIA)** is a U.S. federal law that grants the public the right to request access to records from any federal agency. However, many state and local governments have similar public records laws, which can apply to educational institutions. Under FOIA and state equivalents, public agencies are required to release certain records upon request unless they are exempt.

Here are the main risks for a teacher who uses their personal smartphone to gather and store student data:

1. Inadvertent Exposure of Sensitive Data

- If the teacher's smartphone is considered a device for storing public records (as some public schools or districts may interpret personal devices used for school-related purposes), data on the phone—such as student photos or notes—could be subject to a FOIA request.
- Any student-related information stored on the personal phone, including photos, assessments, or classroom activities, might be considered part of public records and could be requested by anyone under FOIA, depending on local laws and the context in which the data was collected.

2. Privacy Violations and Student Protection

- Student data, including photographs, personal information, or academic records, is protected by laws such as the **Family Educational Rights and Privacy Act (FERPA)**, which prevents the unauthorized release of information without parent or guardian consent. A FOIA request could unintentionally expose this data if not handled properly, violating FERPA regulations.
- Teachers storing sensitive data like photos of students on their personal phones may inadvertently expose this information to others, especially if the phone is not sufficiently secured (e.g., lacking password protection or encryption).

3. Lack of Control Over Data Access

- Personal smartphones may not have the same level of security and data access controls as district-provided devices, which are typically set up with policies and protections around data storage, encryption, and access permissions.
- If the teacher's personal phone is lost, stolen, or hacked, the risk of exposing sensitive student data increases significantly. Without proper safeguards, there could be a breach of privacy that could lead to legal and ethical ramifications.

4. Potential Legal and Disciplinary Consequences

- If a FOIA request for student data stored on a teacher's personal device is made, the teacher could be required to release information they may not have intended to disclose, potentially violating district policies on privacy and confidentiality.
- Schools and districts could discipline teachers who do not adhere to proper protocols for handling student data. For example, storing student data on personal devices may violate policies requiring data to be stored only on school-approved systems that are compliant with privacy laws.

5. Confusion Between Personal and Professional Boundaries

- Teachers using personal smartphones for school-related tasks blur the line between personal and professional use. This can complicate the situation when it comes to legal compliance and responsibility. A teacher may not realize that the data on their phone could be subject to FOIA requests, or they may not be aware of the potential consequences of not following appropriate data protection policies.

Mitigating the Risks

To avoid the potential FOIA and data privacy issues, teachers should:

- **Use school-provided devices** for collecting and storing student data whenever possible. These devices are typically configured with appropriate security protocols and are better aligned with privacy policies.
- **Follow district policies** regarding the storage, handling, and sharing of student information, and make sure any personal devices used for work-related tasks comply with those policies.
- **Secure personal devices** (when allowed to use) with strong passwords, encryption, and regular backups to protect sensitive student data.
- **Obtain proper consent** from parents or guardians before capturing and storing photos or sensitive information about students.
- **Limit personal use** of devices for professional purposes, maintaining clear boundaries between personal and school-related activities.

Governor's Education Emergency Relief