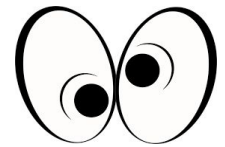


QR,PD,PLC,FUD,FAQ

Apparently, several people are spreading misinformation about using **QR** codes. There is some very real **Fear**, **Uncertainty**, and **Doubt** amongst some of our employees. So, we thought a short **Frequently Asked Question** document would be appropriate.

Recently, the district started using QR codes to streamline the sign-in process for PD and PLC's. The QR codes simply link to a Google Form.

FAQ's



Can you see everything on my phone?

No. Opening a QR code to sign-in to PD simply opens a web site. That's it. This doesn't look at anything on your phone. We do not install anything.

Do I have to use my phone?

No. The district has never said that teachers have to use their phones. Computers have always been available. We have paper sign-in sheets available. The goal is to make things as easy as possible.

Is the information on my phone FOIAble (i.e. FOIA request)?

If you send a work-related e-mail from your phone using a district account, that one particular email would be subject to FOIA laws but not everything on your phone. Please remember that ultimately e-mail is server-based so a FOIA request for e-mail would ultimately require the district to search its servers for the requested information.

Does the District track what I do on my phone?

No. Again, we do not have that ability.

Does Facebook know what I do on my phone?

Yes.

**But we have nothing to do with Facebook.*

*** This part is intended as just a bit of humor (but, yea, if you've installed Facebook on your phone, they probably know a lot about you).*

Why did the district switch to QR codes?

It takes a ton of time, effort and person power to process the handwritten sign-in sheets. Since teachers can now receive SCECH's for PD, Late Starts and more, this can mean multiple (roughly 27 different) sign-in sheets per individual. That is time that could be used supporting teachers in the classroom.



What does the district know about that I do on my phone?

Glad that you asked. First of all, we can only know about your district account. That means that you must sign-in to a program, website, application in order for us to have any information. For example, when you sign-in to the PD attendance sheet, we can know that you've signed-in to the attendance sheet. We do NOT know your Candy Crush score (a total guess that you have Candy Crush installed), we can NOT read your Facebook timeline, we can NOT know which tunes you are jamming to on Spotify.

Here is what the district may know:

- If you sign-in to the Chrome browser (not just Google, but to the actual Chrome browser) with your District Account, information on which web sites that you go to using your District Account will be recorded. *This is expected and useful. If you are signed-in using your District Account, and find something of interest for work, that information is also available to you on your work computer. This is because the information is account-based, not device-based.*
- Any email that you send using your District Account.

* Note that if you sign-in to the Chrome browser using a personal account, we do not have access to any of that information. It is really only your work account that we have a record of.

Thus, it doesn't really matter which device you use. We only know the "stuff" that you do with your Dearborn Public Schools account.

Where does this misinformation come from?

Many people don't really understand what is happening with technology. We can posit a guess as to where this came from. This is part of the FUD.

Several companies have been in the news lately about being able to track you. Google was one of those. Facebook was another.

Facebook has been a particularly "bad actor". They have apologized for the many decisions that they made impacting user privacy data (and then do it again). For example, Facebook recently paid a fine of \$5,000,000,000 (that's \$5 Billion) to the FTC for sharing data without letting people know. Facebook has also installed cookies so that they could track where you go even if you aren't signed into Facebook.

Google is being fined by the EU (European Union) for privacy violations. (The EU recently passed GDPR - General Data Protection Regulation. This is a much more stringent law than what exists in the U.S.) Google's violation was tracking the location of individuals even with "Location History" turned off.

Generally, people sign up for a service and get something in return for something. With a personal Google account (as opposed to a Google account through the district), Google collects a lot of information and provides services. Google aggregates information and shares the aggregate with businesses that want to advertise. Essentially, Google says “Hey, we’ve got a lot of people that really are into camping. Would you like to market to campers?” A camping company might say, “absolutely. Send them our ad for camp stoves”.

In return, users get free email, free searching, the ability to create spreadsheets, documents, mapping services, etc. Lots of people use Google Maps for example. Some people who use Google Maps are surprised that Google “knows where I am”. Given the functionality of Google Maps, knowing where you are is pretty important.

I didn’t really read all this. Can you give me the short version?

Sure. We don’t know what is on your phone.

Using the QR code (or the Bit.ly link) for signing in to PD is just opening a link.