March 2020

COLCHESTER INFORMATION TECHNOLOGY DEPARTMENT

TECHNOLOGY TIDBITS

INSIDE THIS ISSUE:

Posting to Blogger with Email

By Tammi Tandy

There are times when you are out doing GREAT things with your students and you say to yourself, I wish I had a computer so I could post this stuff to my BLOG. Well guess what… you can. You can post to your blog with your phone or iPad while you're out and about by using your email. You simply following these simple instructions below.

First you need to make sure you have email set up on the device. (iPad/Phone)

Next go to your blog and select **Design** and then **Settings.**

In **Settings** choose **Email** and choose **secret Words** (this is where you will enter your private word) and choose **Publish email immediately.** Make sure to Save Settings

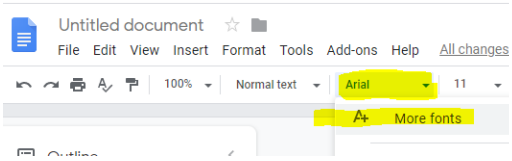
Once you have set up your blog to receive emails you can now take a picture/s and email them to your blog using the email account that you created in blogger and it will post directly to your Blog. The email subject title now becomes your Blog title and any comments in the body of the email now become your post. If you have questions give us a call at 264-5727 Enjoy ☺

More Fonts in a Google Doc

By Richard Bird

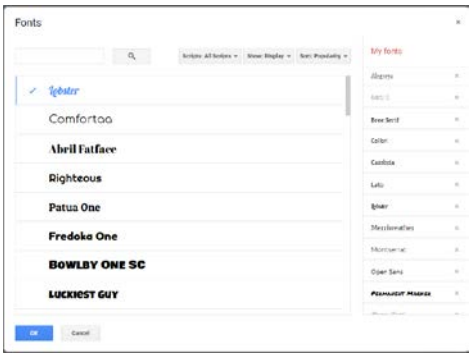
Have you ever been disappointed by the limited number of fonts available in a Google Doc?

Google has the option to use many more fonts than the default few. To access them simply open the fonts dropdown and click More Fonts



This will bring up a window allowing you to choose many more fonts for your documents.

Simply click the font you want and it will become available in your font dropdown.



Phishing Scams – What (not) to do.

By Peter Keenan

Phishing is a form of social engineering where an attacker uses social skills to obtain or compromise information about an organization or individual. The attacker poses as someone you may know or representing an entity you may be familiar with like a bank, a credit card company or a charity organization. Phishing attacks may come from other types of organization also and may try to take advantage of current events or certain times of the year, such as

- Natural disasters (e.g., Hurricane Katrina, Indonesian tsunami)
- Epidemics and health scares (e.g., H1N1)
- Economic concerns (e.g., IRS scams)
- Major political elections
- Holidays

Other forms of this type of attack are “vishing” – using a telephone call, “smishing” – using SMS or text messages and “whaling”, using administrative or well know email addresses as the sender’s email address to prompt attention and increase the likelihood of a reply.

Internally the district has experienced phishing attempts as emails appearing to be from school administrators to employees asking for information or documents. Google is pretty good at tagging these as suspicious but occasional they do get delivered to an inbox and not tagged as spam or suspicious. In these cases usually there are dozens of emails in the attempt directed at numerous random internal email addresses which have been obtained from the web. If you do receive something like this the first step is to ask yourself -

Do I know the person that contacted me, or do I have a relationship with the organization sending the email?

If the answer is “No,” it could be a phishing scam. **Delete it.**

If the answer is “Yes,” contact the individual or organization by email using a known good email address (don’t use reply) or call using a phone number you know is real - **not the information presented in the email**.

- ✓ Never send confidential information in an email.
- ✓ Be very careful about replying to emails asking you to confirm or update any information about an account.
- ✓ Be careful about opening or saving documents or attachments that come with an unknown email. Do not trust these kinds of emails even if they appear to be sent by some authorized entity.

If you think you may have accidentally revealed sensitive information

- ✓ Report it to the IT department.
- ✓ If you believe your financial accounts may be compromised, contact your financial institution immediately. Watch for any unexplainable charges to your account.
- ✓ Immediately change any passwords you might have revealed. If you use the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.

More information on this topic is available from the National Cyber Awareness System website at https://www.us-cert.gov/ncas/tips/ST04-014

Accessing the internet offsite

By Chris Whittaker

Are you off site and trying to access the internet at a conference or a hotel and you're not getting a connection to the internet with your district device? This may be due to certain devices/browsers only allowing you to access SSL websites. Browsers typically have this in place to keep you protected from unsecure websites, but these policies also tend to block the captive portal pop-up, that you need to access, in order to log in to the wireless network.

To bypass this policy, and allow the captive portal to prompt, open a browser (Chrome, IE, Edge, Etc.) and go to http://neverssl.com/ This will redirect you to the establishments wireless login page. Simply log in with the username and password you were given, and you should be able to start browsing the internet!

If this doesn't work, please give us a call at 264-5727.

OneDrive

By Jeremie Paquette

Tips and Tricks to using OneDrive

Accessing your OneDrive:

Use File Explorer → OneDrive – csdvt.org
Onedrive.com → login with school account

Icons and their meaning:

Online only files

When you open an online-only file, it downloads to your device and becomes a locally available file → can become an online file only again.

Only files that you mark as "always keep on this device" will look like this. This will take up space on your device, but always there if your offline.

Version History

Log onto Onedrive.com, right click on a file and select version history. Select the version date you want to restore.

As a reminder, please do not share files – these are your personal files.

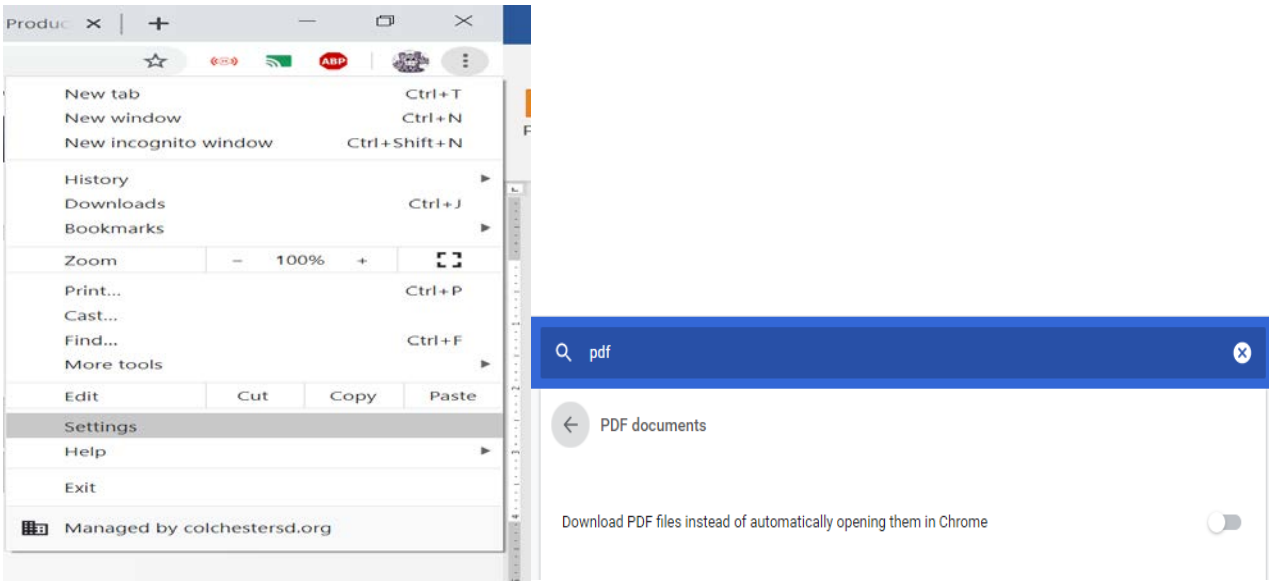
To share, we are using Share Point or S: Shared Drive or Google Drive Team Sharing.

Opening PDFs in your browser

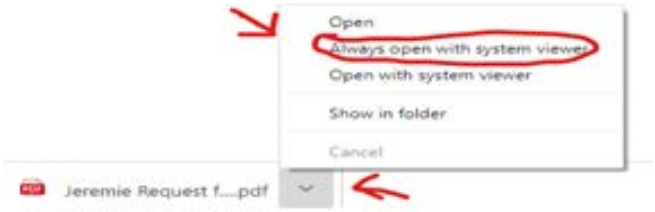
By Jared Brunelle

If you're tired of your pdf documents downloading, and you would rather them open with one click, you came to the right article!

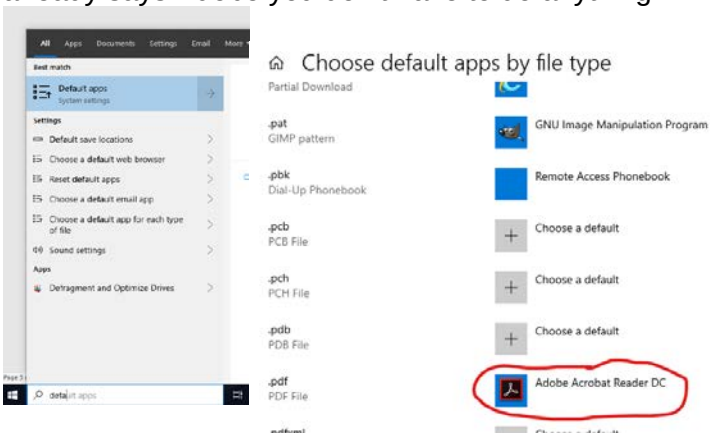
The first step is to go to your Chrome browser. If you click on settings and search "pdf" you'll get this option as a result (pictured below). Make sure this is turned off.

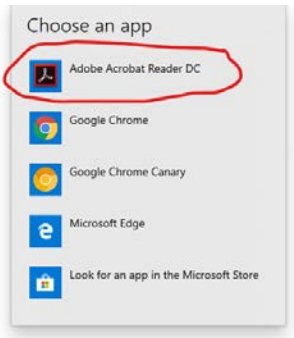


One other thing you'll need to change is when you see the pdf download on the bottom of the browser, you'll want to hit the dropdown menu and click "Always open with system viewer".



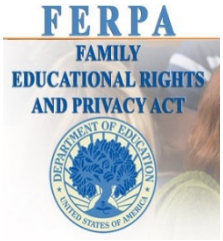
You'll also want to search "default apps" in the bottom left near the windows icon, then click on "choose default apps by file type". Once on that screen scroll all the way down to PDF and click on it to change it from edge to Adobe acrobat, if it already says Adobe you don't have to do anything.





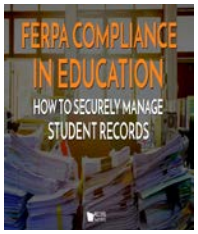
FERPA Overview

By Trevor Lombard



FERPA is a federal privacy law that affords parents the rights to have access to their children's education records, seek to have the records amended, and consent to the disclosure of personally identifiable information from education records, except as provided by law. Under FERPA, "Parent" is defined as parent of a student and includes natural parent, legal guardian, or someone acting as a parent in the absence of the actual parent/guardian. There are legal exceptions to this if warrants are presented or if there is custodial agreements in place.

There is a lot of nuance when it comes to enforcing FERPA and there are no hard and fast rules that will apply to all scenarios, but all Powerschool users should be aware of FERPA when it comes to disclosing information. Here are a couple scenarios that illustrate how this comes into play:



Scenario 1- A law enforcement officer comes to the front office at the high school and asks the person working if a certain student was in school that day because he needed to ask them a question. The person working has seen the student in the hallway earlier and lets the officer know that the student is present today; this is acceptable under FERPA. If the front desk person has not seen the student and they have to pull up the record in Powerschool to check attendance, this becomes a situation where they would be divulging information from the student's education records to a non-parent and this would not be allowed under FERPA.

Scenario 2 – A teacher wants to post exam grades for a class in the hallway and the report they are posting them from excludes student names, but includes gender, race, and other demographic information that could identify a student. Even without the names showing, if you are able to identify a student based on other info then this is a FERPA violation. For example, since race and gender are shown, if there is only a single black female in the class their grade can be easily identified.

These are some of the simpler scenarios in which FERPA can be applied, but it can be much more complex. If there are any questions about anything FERPA related don't hesitate to reach out at x5761 or at trevor.lombard@colchestersd.org.