FOIA, LITIGATION, AND EDISCOVERY OH MY!

Chris Thomas

Endpoint and Cloud Systems Architect

Ingham Intermediate School District

cthomas@inghamisd.org

@AutomateMyStuff

Ingham Intermediate School District
A Regional Educational Service Agency

SESSION DESCRIPTION

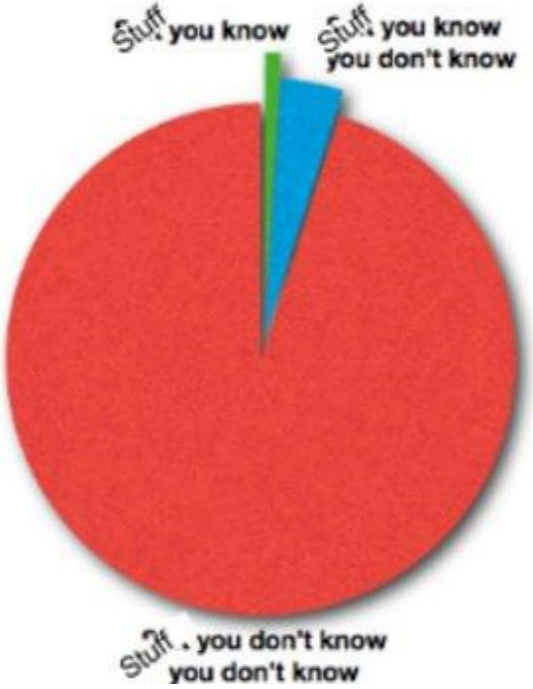
- Come join our roundtable discussion on all things FOIA, Litigation, eDiscovery, student/staff investigations … Hopefully you've been lucky enough to not have had to deal with these things often … so those of us who HAVE will share with you some tips, tricks, gotchas, and CYA's. Audience participation strongly encouraged … we're better, faster, stronger together!
  <NOTE: Roundtable/Panel Discussion>

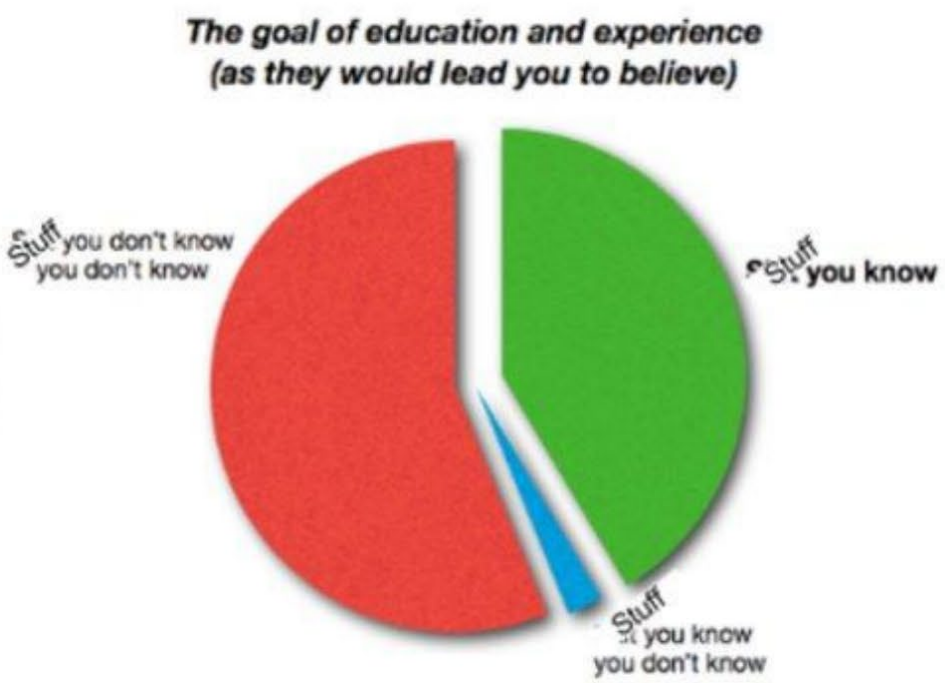
INTRODUCTION

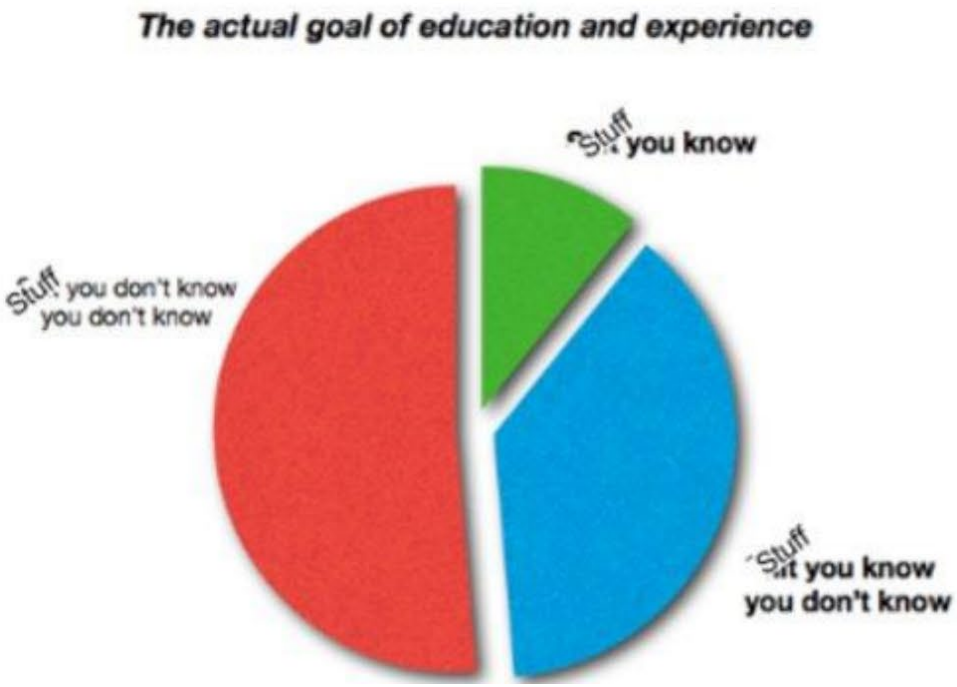
- 27-ISH YEARS OF EXPERIENCE IN K-12 TECH
  - Junior/Senior year as an Intern for Huron Valley Schools
  - 7-ish years as a Computer Repair Technician for Bloomfield Hills Schools
  - 8-ish years as a Technical Systems Coordinator for Bloomfield Hills Schools
  - 9-ish years as a Desktop Engineer for Ingham ISD
  - Few months as an Endpoint and Cloud Systems Architect for Ingham ISD
- MAEDS BOARD MEMBER AND FREQUENT PRESENTER SINCE 2014
- MISCUG BOARD PRESIDENT AND ORGANIZER
- MMSMOA PAST PRESENTER

IMPOSTER SYNDROME

https://www.bridge-global.com/blog/3-types-of-knowledge/







TEMPERATURE CHECK

- SHOW OF HANDS …
  - How many have had to work on FOIA requests?
  - How many have had to work on litigation/subpoenas?
  - How many have worked with local sheriff's office and/or FBI?

GENERALLY SPEAKING…

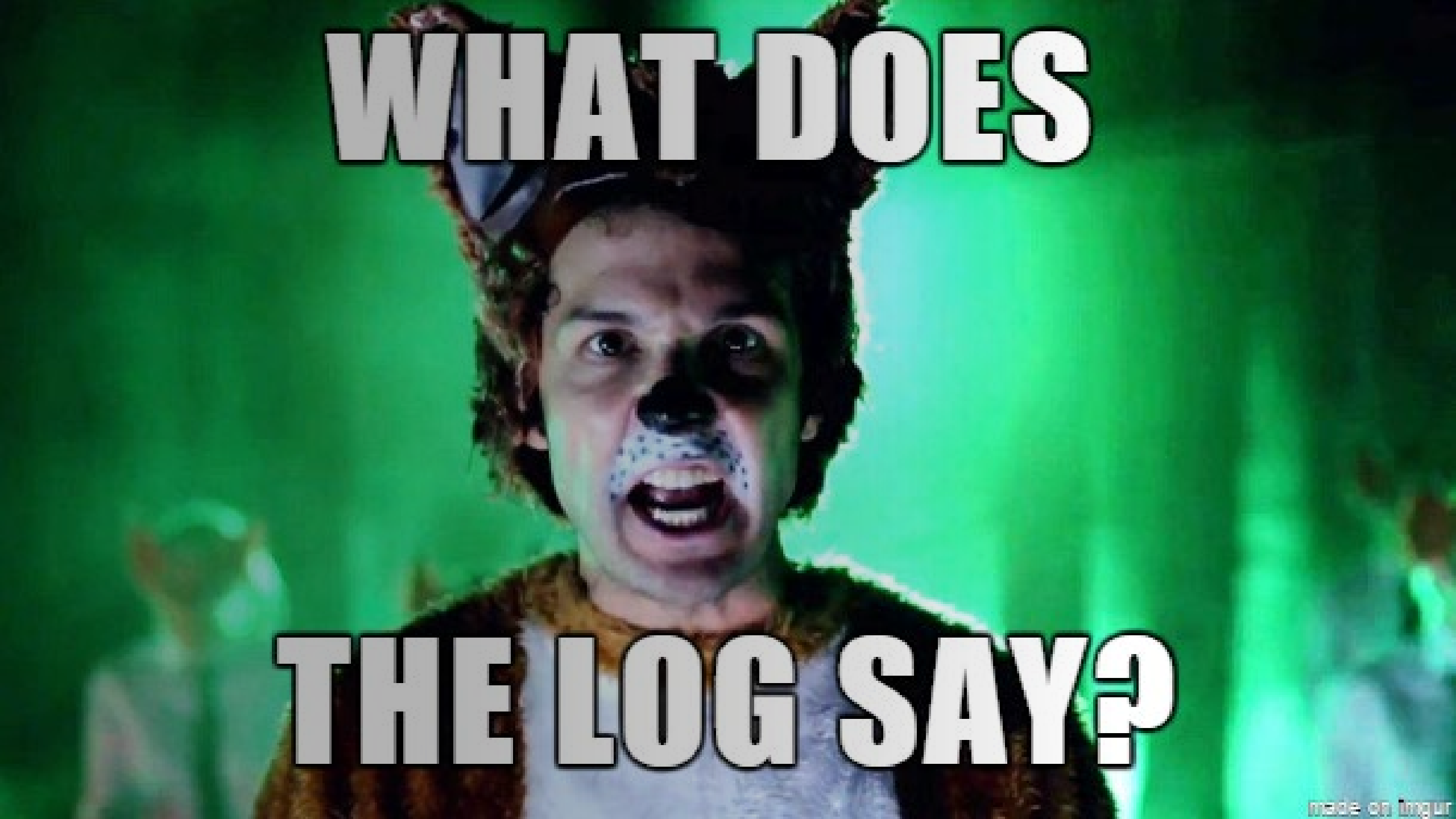
- Depending on FOIA language/search terms you might need to clarify with district leadership if you should do the efforts or just give an estimate of time to allow the requestor to put a deposit down (if charged) or if requestor wants to reframe their query to be less effort/broad
  - Usually search exactly what they asked for, unless leadership says otherwise
    - (ex: 'School <District Name> Resource Program' request vs. you know it internally referred to as 'SRO')
    - (ex: 'Chris Thomas' request vs. you know it was noted as 'CT' in notes)
  - Sometimes district leadership/law firm might believe you should search all variants you are aware of
- A 'correspondence' is email … if a memo was created in OneDrive/Google Drive, it should have been emailed so it would be captured in that search/export
- If you support Google and Microsoft cloud … you unfortunately have to search both locations

CYA

- Verify staff-related requests are approved by HR/Superintendent
- Build a 'narrative' based on logs/data instead of just dumping raw files on admins/requestors
- Even if something is sensitive and confidential … request a ticket or email with generic language for the actions
- Keep good notes, even if only for yourself, in case any questions of what/how/why you did what you did
- Sometimes you'll work on investigations that your boss or your bosses boss don't have any details to, but generally let them know you're busy with an investigation so they know your availability

INCIDENT EXAMPLES

- Cyberbullying Between Students
- Self-Inflicted Cyberbullying For Attention
- Inappropriate Emails
- Unwanted Messages
- Profile Image Changing
- Student Runs Away
- Colleague Changes Settings Without Informing The Team
- Colleague Changes Settings But You Forgot That They Informed The Team
- YOU Changed Settings But Forgot To Inform The Team


WHAT DOES
THE LOG SAY?
made on imgur

AUDIT LOGS

Microsoft

- Off by default
  - Turn auditing on or off
- https://purview.microsoft.com/audit
  - Search the audit log
  - Manage mailbox auditing

Google

- On by default
- https://admin.google.com/ac/sc/investigation

EMAIL LOG SEARCH

Microsoft

- Exchange > Mail Flow > Message Trace
- Email & Collaboration > Threat Explorer
- Review > Quarantine

Google

- Reporting > Email Log Search
- Reporting > Audit & Investigation > Gmail Log Search
- Reporting > Audit & Investigation > Gmail Messages
  - Paid license only
- Apps > Google Workspace > Settings for Gmail > Manage Quarantines

EDISCOVERY

Microsoft

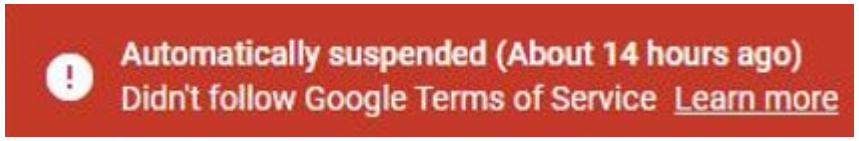
- Microsoft Purview eDiscovery solutions
- Microsoft Purview > eDiscovery > Cases

Google

- Vault – Admin Help
- Google Vault > Matters

EDISCOVERY CAVEAT - RETENTION IS NOT A BACKUP

- Scenario:
  - User creates ticket indicating that a student account cannot login to their Chromebook or any Google services, like Google Classroom or Google Meet.
  - Help Desk validates student account is suspended, but they are unable to unsuspend the account.
  - You engage Google Support to find that they cannot unsuspend the account and must escalate. Yet, escalations will give you no explanation.
  - Whatever, let's make a new student account and recover their data from eDiscovery / Google Vault.



GOOGLE DOCS/SLIDES/SHEETS COMPLICATIONS

- eDiscovery/Export of Doc/Slide/Sheet is MOMENT-IN-TIME version
- Need permissions to file to view revision history
  - Do not email/share/print/download version history if any CSAM exists in the file. Ask Sheriff office to meet with you in person.
- Learn to 'expunge' from Vault retention policy
- gam user student.one@students.inghamisd.org show filelist
- gam user student.one@students.inghamisd.org add drivefileacl <id> user cthomas@inghamisd.org role editor
- Review 'revision history' taking notes as-needed
- gam user student.one@students.inghamisd.org delete drivefileacl <id> cthomas@inghamisd.org

GOOGLE DRIVE FOLDER SEARCHING/PERMISSIONS

- gam user student.one@students.inghamisd.org show filelist
  - Result will show 'folders' in 'webviewlink'

```
c:\GAM7>gam user student.one@students.inghamisd.org show filelist
Getting all Drive Files/Folders that match query ('me' in owners) for student.one@students.inghamisd.org
Got 3 Drive Files/Folders that matched query ('me' in owners) for student.one@students.inghamisd.org...
Owner,name,webViewLink
student.one@students.inghamisd.org,CT - Notes,https://docs.google.com/document/d/1NF_LnN0YsyG_Yno4vvKlgq88IQO7yQfsdLXBOt
OCMjM/edit?usp=drivesdk
student.one@students.inghamisd.org,Title IX,https://drive.google.com/drive/folders/13NRPZgQ-J6ghWA7TId9buIEqXpjqsrE6
student.one@students.inghamisd.org,SecretSlides,https://docs.google.com/presentation/d/1u137emI_9_OH-n1wgyf9rinkQ_eSdVam
btt9oBqzdcg/edit?usp=drivesdk
```

- gam user student.one@students.inghamisd.org show filetree
  - Result will show visual depth of folders/files

```
c:\GAM7>gam user student.one@students.inghamisd.org show filetree
Getting all Drive Files/Folders that match query ('me' in owners) for student.one@students.inghamisd.org
Got 3 Drive Files/Folders that matched query ('me' in owners) for student.one@students.inghamisd.org...
User: student.one@students.inghamisd.org, Show 1 Drive File/Folder
  My Drive
    Title IX
      CT - Notes
    SecretSlides
```

GOOGLE DRIVE FOLDER SEARCHING/PERMISSIONS

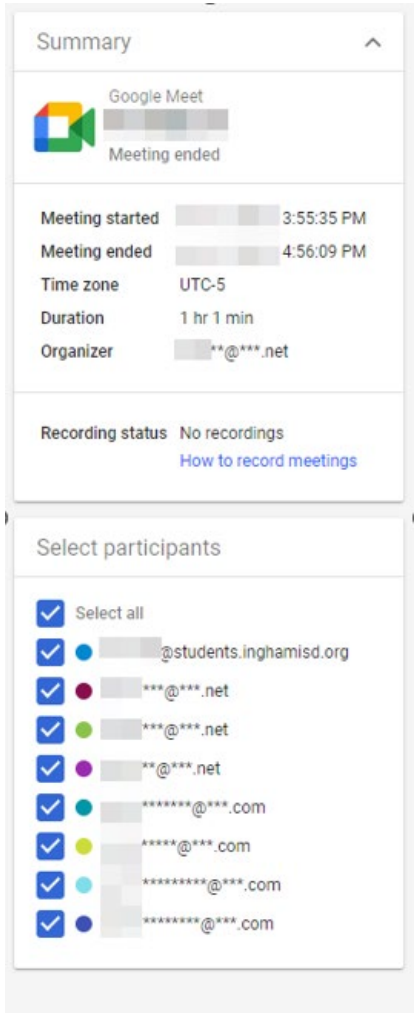
- Need: User is on leave, but district needs notes from a Title IX investigation
  - Add someone as editor to a folder
    - gam user student.one@students.inghamisd.org add drivefileacl <id> user cthomas@inghamisd.org role editor
  - Review files and folders.
  - Have editor add more editors to files/folders as-needed for situation
  - Remove someone as editor to a folder
    - gam user student.one@students.inghamisd.org delete drivefileacl <id> cthomas@inghamisd.org

YOUTUBE - CAUTION ADVISED

- No Vault / eDiscovery
  - No retention of data
- Lack of administrative tools other than approved videos feature.
- Limited support as an "Additional Google services"
  - Should lean into 'Brand Accounts' to ensure videos exist when a user leaves org.
- Curriculum ONLY stored in YouTube?
  - What do you do if a user violates TOS and gets account suspended as I mentioned earlier?
  - What do you do if a user accidentally deletes videos?
  - What do you do if a disgruntled user deletes videos and/or channel on purpose?

GOOGLE MEET

- Pay attention to 'Meet safety settings' and 'Access'
  - 'Meetings created in your organization only'
    - Probably the most ideal setting for students
      - Complicated if LEA students use Google Meet with ISD/RESA staff
  - 'Meetings created in any Workspace organization'
    - Good luck, might as well be full open if other orgs don't control if their students can create a Meet call
  - 'Any meetings, including meetings created with personal accounts'
    - I can't think of a single reason that a student would need this setting



ACRONYMS/SLANG

- **AITR**: Adults In The Room
- **POS**: Parents Over Shoulder
- **KYS**: Kill Yourself
- **KMS**: Kill Myself
- **KMN**: Kill Me Now
- **THOT**: That Ho Over There
- **TDTM**: Talk Dirty To Me
- **WUD/WYD**: What You Doing?
- **53X**: Sex
- **BAE**: significant other, "before anyone else"
- **BET**: "yes" or "watch me"
- **GHOST**: purposely ignore someone
- **TROLL(ING)**: intentional harassment, criticizing or antagonizing of someone
- **SWAT(ING)**: making a false report to elicit response from law enforcement
- **CATFISHING**: fake identity to target a victim online
- **IMPING**: Impersonating someone online in order to embarrass them
- **SALTY**: Someone upset by something

EMOJIS/KAOMOJI

- CHROMEBOOK
  - https://support.google.com/chromebook/answer/6076237?hl=en#zippy=%2Cinsert-emoji-or-other-images
- WINDOWS 10
  - https://support.microsoft.com/en-us/windows/windows-10-keyboard-tips-and-tricks-588e0b72-0fff-6d3f-aeee-6e5116097942
- IOS
  - https://support.apple.com/en-us/HT202332
- ANDROID
  - https://support.google.com/gboard/answer/2842292?co=GENIE.Platform%3DAndroid&hl=en

- THREATENING
  - 👊 👉 🚑 🔪 🔫 💀
- RACISM
  - 🍉 🍗 🐵 👌
- SEXUAL
  - 👄 ✊ 💦 🍆 🍑 😈 🌮
- RISKY/ILLEGAL
  - 🍁 🥦 💊 💉 🦽
- KAOMOJI
  - (ﾉ°□°)ﾉ ⌒┻━┻
  - (　-_･)▄▅デ═一 ▸

Q&A / COMMENTS