



Ethics of Technology Use

Dan Florell, Ph.D., NCSP

Eastern Kentucky University
Richmond, Kentucky

Texas Association of School Psychologist
Annual Convention – Houston, TX
November 5, 2022



1

Goals

- Think ahead to prevent issues/problems
- Become more aware of technology and ethical issues surrounding use of various technologies
- Ask questions about your daily practices
- Refer to Laws and NASP Ethics in 2020 Professional Standards
- Make a plan
- Think “Best Practices”
- Technological Competence



2

School Laws and Digital Records State Law

THE STATE STUDENT PRIVACY REPORT CARD

FIGURE 3 - STATE GRADES BY CATEGORY

State Name	Parties Covered & Regulated	Transparency	Parental & Student Rights	Commercial Uses	Data Security	Oversight & Enforcement	Other Provisions	Overall Grade
Tennessee	C+	C	B	B-	B-	C-	C+	B-
★ Texas	D+	F	D+	C	D	F	F	D+
Utah	C	C+	C-	D	C+	C	D-	C
Vermont	F	F	F	F	F	F	F	F
Virginia	B-	D	C	B-	C	D	D-	C+

Source: Parent Coalition for Student Privacy (January, 2019). The State Student Privacy Report Card: Grading the States on Protecting Student Data Privacy.

3

School Laws and Digital Records

- Family Educational Rights and Privacy Act (FERPA)
 - FERPA was enacted in 1974 and provides certain minimum privacy protections for educational records.
 - FERPA was passed to protect the privacy of student educational records by regulating to whom and under what circumstances those records may be disclosed.
 - FERPA applies to educational agencies and institutions that receive federal funds administered by the Secretary of Education.



4

School Laws and Digital Records

- The Protection of Pupil Rights Amendment (Hatch Amendment of 1978) updated 2001
 - Applies to state or local education agencies that receive funding from the United States Department of Education.
 - Specifically, it ensures the rights of students and parents surrounding the collection and use of information for marketing purposes as well as information regarding certain physical exams.

5



Internet Laws and Digital Records

- Children's Online Privacy Protection Act of 1998 (COPPA)
 - Empowers the FTC to regulate the operators of commercial websites or online services targeted to children in the collection and use of personal information obtained from children. COPPA defines "personal information" to include
 - (1) a first and last name; (2) an address; (3) an e-mail address; (4) a telephone number; (5) a Social Security number; or (6) any other identifier that the FTC may determine permits the physical or online contacting of a specific individual.
 - If a website is directed at children or the operator knowingly collects personal information from children under 13, COPPA requires that the website obtain parental notice and consent.



6



Requirements

- COPPA-covered operators must:
 - Post “clear and comprehensive” online-privacy policy.
 - Give parents “direct notice” before collecting information from children under 13.
 - Obtain “verifiable parental consent” before collecting such information.
 - Allow parents to review their children’s information and request that it be deleted.

7



Requirements

- COPPA-covered operators must:
 - Allow parents to opt out of further collection, use, or sharing of information pertaining to their child.
 - Maintain the confidentiality and security of any child’s information that is collected.
 - Delete children’s information after it is “no longer necessary to fulfill the purpose for which it was collected.”

8



Parent Consent

- Federal Trade Commission - under certain circumstances, “schools may act as the parent’s agent and can consent to the collection of kids’ information on the parent’s behalf.”

9




Parent Consent

- Law requires parental notification
- FTC expects companies to publicly post a privacy policy that includes:
 - Descriptions of what information is collected from children.
 - How information may be used and disclosed.
 - Contact information for any third parties that may also be collecting information through the site, and more.
- Schools expected to make such notices available to parents.

10

Health Laws and Digital Records

- Health Insurance Portability and Accountability Act (HIPAA) 
 - “Covered entity,” health plan, healthcare clearinghouse, or any healthcare provider who transmits health information in electronic form in connection with transactions for which Secretary of HHS has adopted standards under HIPAA.
 - School that is not covered by FERPA may be covered entity if it provides health services for which it transmits health information electronically, such as submitting claims for payment from a health plan.

11

Health Laws and Digital Records

- Health Information Technology for Economic and Clinical Health Act (HITECH) – Part D Privacy
 - Requires [HIPAA](#) covered entities to report data breaches affecting 500 or more individuals to [HHS](#) and the media, in addition to notifying the affected individuals.
 - This subtitle extends the complete Privacy and Security Provisions of HIPAA to business associates of covered entities.
 - New rules for the accounting of disclosures of a patient's health information. It extends the current accounting for disclosure requirements to information that is used to carry out treatment, payment and health care operations when an organization is using an [electronic health record](#) (EHR).

12

Updated Federal Guidance

- Clarify HIPAA and FERPA for student records

Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) And the Health Insurance Portability and Accountability Act of 1996 (HIPAA) To Student Health Records



U.S. Department of Education



U.S. Department of Health and Human Services

13



U.S. Department of Education

Head Spinning Regulations

- US Dept. of Education has offered some help
- Protecting Student Privacy
 - Offers guidance to school regarding the various laws regarding student privacy and confidentiality
 - <https://studentprivacy.ed.gov/>



14

Tech Ethics Questions to Ask

- Most tech ethics questions center on confidentiality and privacy and the impact it has on the client's well being.
 - Who owns the information?
 - Where is the information being stored?
 - How is the information being stored?
 - How long is that information going to be stored?
 - Who has access to the information?
 - What safeguards are in place?

15

K-12 Cyber Incidents

From 1/1/16 to 2/18/22
1331 Incidents

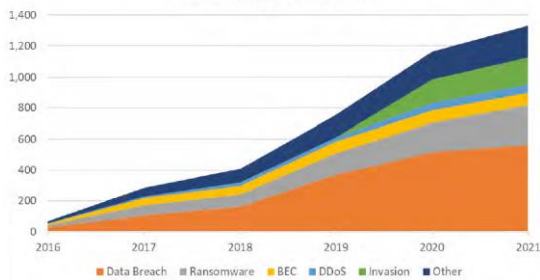


- Purple – Data Breaches/Leaks
- Yellow – Ransomware
- Blue – Phishing
- Green – Denial of Service
- Red – Other Incidents

16

K-12 Ransomware

Number of Publicly-Disclosed K-12 Cyber Incidents by Incident Type: 2016-2021



17

Dive into School Ransomware

- Double extortion of school districts
 - With this tactic, ransomware actors steal victim’s data before their malware strain activates its encryption routine. They then have option of demanding two ransoms.
 - First one is the provision of a decryption utility.
 - Second one guarantees verbal confirmation of having deleted victim’s data from their servers. They can also leverage that data theft to pressure victims — even those that have a robust data backup strategy.

18

Dive into School Ransomware



- Experience of Weslaco Independent School District (TX), late 2020 victim of ransomware attack, typical of double extortion tactic:
 - ...the hackers, spurned by Weslaco’s decision to not pay, dumped the files they pilfered on their website. One of those, still posted online, is an Excel spreadsheet titled “Basic student information” that has a list of approximately 16,000 students, roughly the combined student population of Weslaco’s 20 schools last year. It lists students by name and includes entries for their date of birth, race, Social Security number and gender, as well as whether they’re an immigrant, homeless, marked as economically disadvantaged and if they’ve been flagged as potentially dyslexic.

19

Best of Intentions

- Even when school psychologists create concrete guidelines around areas of self-disclosure, the Internet can counteract even best of intentions.
- Issue continue to increase in relevance for ethics as boundaries blurs between public and private lives.

20

Basic Risk Management



- **Standard of Care:** Reasonable and Prudent
- Psychologist
 - **Judicial:** How similarly qualified practitioners would have managed the patient's care under the same or similar circumstances
 - Must have and use the knowledge ordinarily possessed by members of the profession in good standing
 - **Ethical:** As used in this Ethics Code, the term
 - **reasonable** means the prevailing professional judgment of psychologists engaged in similar activities in similar circumstances, given the knowledge the psychologist had or should have had at the time.

From: J. Younggren, 2013

21

Three Keys to Success in Risk Management

- **Informed Consent** – records including electronic transmission and storage
- **Appropriate consultation** – with others
- Good **record keeping** practices and strategies



22



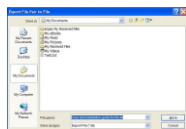
Ethics, Risk Management & Technology

- It can get you in trouble, if you “mess up”
- Ignorance is not BLISS – “Standard of Care”
- Professional ethics and technology do overlap
- If in doubt – pause or ask a colleague

23

Ethics, Risk Management & Technology

- **Copiers** – may store your copies
- **E-mails** are open and available to everyone
- **Master files/reports** – access issues
- **“Other files”** – not protected/computer access; file names may be viewed



24

Ethics, Risk Management & Technology



• Data management

- Storage
 - Cloud
 - CD/DVD/external hard drive
- Lost data/computer/USB data stick
- Password protect it – folders and files
 - ENCRYPTION!!!



25

Steps in Protecting Student Data

- Conduct a structured analysis of various risks student data could experience.
- Take measures to protect against these security risks
- Protection is a moving target which needs regular updating



26

Steps in Protecting Student Data

• Basics:

- Take advantage of built-in safeguards in storage programs.
 - Eg. Administrator limiting access to information based on need to know.
- Maintain minimal clinical records



27

Steps in Protecting Student Data

• Systems:

- Create comprehensive inventories of types of student data collected
- Develop clear record storage and disposal policies
- Learn and employ technical best practice



28

Best Practices – Technical Competence

- School Psychologists be part of decision-making process about technology
- Develop school policies about technology, assessment, and records management
- Develop consent forms for parents and teachers about technology and data management
- Monitor business agreements between software companies and schools; 3rd Party Vendors



29

Technical Competence

- Keep hardware and software updated
- Protect data and records
 - Encryption
- Be knowledgeable about new laws, regulations, and ethical principles



30

Tech & Ethics Overview

- APA does NOT have specific guidelines for ethical use of technology.
- **APA – General Principles:**
 - Privacy and Security, Competence
 - Confidentiality
 - Nonmaleficence
 - Informed Consent
 - Safety (self-disclosure)
- APA Guidelines for Telepsychology (July, 2013)
- Professional roles v. personal roles in social media



31



NASP 2020 Ethical Code



- Increased attention to digital information
- Guidance on social media use
- Reality of assessment with digital and cloud services

32



NASP Ethics Problem Solving Model

- Use systematic problem-solving process
 - Identify ethical issue involved
 - Consult ethic principles
 - Consult colleagues with greater expertise
 - Evaluate the rights and welfare of all affected parties
 - Consider alternative solutions and their consequences
 - Accepting responsibility for the decisions made

33



Scenario

- A student has been referred for an evaluation. The school psychologist assesses intelligence and academic achievement of student.
- Assessment results are scored through 3rd party cloud scoring software.
- These are uploaded to school’s cloud student record system.

34



Record Keeping Std. II.4.1

- School psychologists safeguard the privacy of school psychological records, ensure parents’ access to the records of their own child, and ensure the access rights of adult students or otherwise eligible students to their own records.
- Parents and adult students are notified of the electronic storage and transmission of personally identifiable school psychological records and the associated risks to privacy.

35



Record Keeping Std. II.4.6

- To the extent that school psychological records are *under their control*, school psychologists ensure that only those school personnel who have a legitimate educational interest in a student are given access to that student’s school psychological records without prior parental permission or the permission of an adult student.
 - This standard *applies to access to physical and electronic records.*

36



Record Keeping Std. II.4.7

- To the extent that school psychological records are *under their control*, school psychologists *protect electronic files from unauthorized release or modification* (e.g., by using passwords and encryption), and they take reasonable steps to ensure that school psychological records are not lost due to equipment failure.

37



Record Keeping Std. II.4.9

- They advocate for school district policies and practices that
 - *Identify timelines for the periodic review and disposal of outdated school psychological records* that are consistent with law and sound professional practice
 - Seek parental or other appropriate permission prior to the *destruction or deletion* of obsolete school psychological records of current students
 - Ensure that obsolete school psychology records are destroyed or deleted in away that the information cannot be recovered.
- In addition, school psychologists advocate for a school service delivery system in which working (not final) *drafts of documents are not stored as student education records.*

38



Texas School Record Laws

- Retention periods listed in this schedule apply to records in any medium. **If records are stored electronically, they must remain available and accessible until the retention period assigned by this schedule,** along with any hardware or software required to access or read them. **Electronic records may include electronic mail (e-mail), websites, electronic publications, or any other machine-readable format.** Paper or microfilm copies may be retained in lieu of electronic records.
- The **use of social media applications may create public records.** Any content (messages, posts, photographs, videos, etc.) created or received using a social media application may be considered records and should be managed appropriately. The retention of social media records is based on content and function. Local governments will need to consult the relevant records retention schedule for the minimum retention periods.

39



Texas School Record Laws

- Section 3-1: Special Education Program Records
 - Student Records - **SD3250-02**
 - **Description** - Records of each student referred to or receiving special education services, including referral, **assessment, and reevaluation reports**; enrollment and eligibility forms; admission, review, and dismissal (ARD) and transitional planning committee documentation; individual educational plans (IEP) and individual transitional plans (ITP); parental consent forms for testing and placement; and other records of services required under federal and state regulation. Includes records of students receiving School Health and Related Services (SHARS); see [Texas Medicaid Provider Procedures Manual](#).
 - **Retention Period** - **Cessation of services + 5 years**, but see retention note (a).
 - **Remarks - Retention Notes:** a) It is an exception to the retention period given for this record group, that the following information must be retained **PERMANENTLY** in some form on each student in grades 9-12 participating in a special education program: name, last known address, student ID or Social Security number, grades, classes attended, and grade level and year completed. If an academic achievement record (see item number SD3200-01(a)) is created for the student and maintained among those for students in the regular population, it is not necessary for special education records custodians to maintain the prescribed information beyond 5 years after the cessation of services, provided that it is contained in the Academic Achievement Record.
 - b) **Prior to the destruction of any records in this record group, the eligible student or the parents of the student, as applicable, must be notified in accordance with federal regulation.**

40



Texas School Record Laws

- Section 3-4&5: Section 504 & Dyslexia Program Records
 - Student Records - **SD3250-20 / SD3250-27**
 - **Description** - Records of each student referred to or receiving services under Section 504, including referral, pre-placement, and **reevaluation reports**; parental notices; group and impartial hearing deliberations; and other records of services required under Section 504 regulations.
 - **Retention Period** - **Cessation of services + 5 years**, but see retention note (a).
 - **Remarks - Retention Notes:** b) **Prior to the destruction of any records in this record group, the eligible student or the parents of the student, as applicable, must be notified in accordance with federal regulation.**
 - **Description** -Records of each student referred to or receiving dyslexia program services, including referral and **assessment reports**; group deliberations; parental notices; and other records of services required under state regulation.
 - **Retention Period** - **Cessation of services + 5 years**, but see retention note (a).
 - **Remarks - Retention Notes:** This record group does not include the special education records of students with dyslexia or related disorders receiving special education services.

41

What is a Digital Record?

- Written notes
- Digitized/Scanned files or reports; records
- Email
- Text/SMS messages
- Audio files
- Video files



42

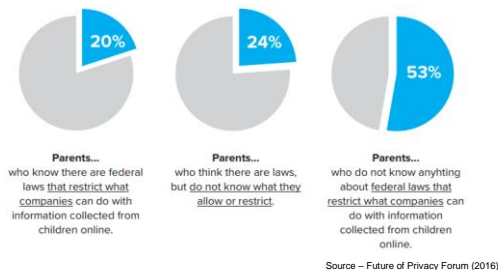


- **HIPAA - Privacy Rule** intentional disclosure of **PHI** & **Security Rule** unintentional or malicious disclosure or loss of record (only electronic records). No mandated protection methods under the law. "**reasonableness**" feature under ethics.
 - Examples: passwords, digital signatures, firewalls, data encryption, encryption over public networks, backup systems, and disaster recovery plan.
- Check email address before responding; reply all
- Remote services – across state lines
- Billing issues – need to know and who have signed agreements with 3rd party billing authority

43

What Do Parents Know?

- Existing Laws



44



Parent Concerns

- Parents comfortable with properly protected electronic education record being created for their children (71%)
- Parents more likely to support collecting and using data in electronic record if:
 - Know school required to ensure security (82%)
 - School required to use electronic education record only for education purposes (84%).

Source – Future of Privacy Forum (2016)

45

Parent Concerns



- Parents have security and privacy concerns, primarily that:
 - Child’s electronic education record could be hacked or stolen (84%)
 - Electronic education record could be used against their child by college or employer (68%).
 - Nearly all parents (94%) believe they should be informed with whom and for what purpose their child’s record is being shared.

Source – Future of Privacy Forum (2016)

46



Informed Consent Std. I.1.1

- Ongoing process
 - Reopen when significant changes in services made
 - Use of technology likely to require revision of consent
- Required
 - When consultation is likely extensive and ongoing
 - If school activities are significant intrusion on student or family privacy

47

Sample Language to Use



- Reference IDEA, FERPA, and HIPAA
 - HIPAA language may be optional
- Section
 - Type of Information We Collect and How We Collect It
 - Includes definition of Personally Identifiable Information (PII)
 - Effective Date and Changes to Privacy Notice

48



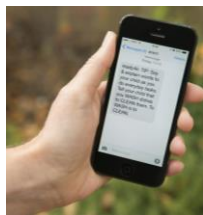
Sample Language to Use

- Section
 - Outline Parent Rights re: Child Records
 - List types and location of information
 - List whom information has been shared with
 - Ask to limit what we share
 - Request communication method
 - Other use of information and withdraw of consent
 - Filing a complaint
 - Uses of records by district
 - When share information without prior consent

49

Home-School Communication

- Convenience: Make it easy for parents to get information in way most convenient.
- Push, not search: Don't make parents search for information, push it out to them.
- Personalized, not standardized: Give parents information appropriate and applicable for their child, class, grade level, and school.



50

Home-School Communication

- Timeliness: Make sure information being communicated is timely and current.
- Realization of busyness: Realize parents are busy and need communications to be concise, to the point, and relevant.
- High impact/high ROI information: Make sure information providing is actionable for parents and important for them to know.



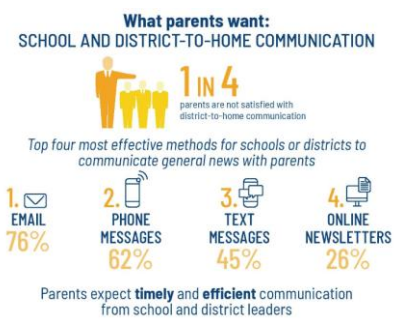
51

Best Way to Contact Parents for Teachers



52

Best Way to Contact Parents for Schools



53

Preferred Social Media of Parents

Table 3: Social media tools cited by parents of school-aged children as used "all the time + often"

SOCIAL MEDIA	PARENTS 29 OR YOUNGER IN AGE	PARENTS 30-39 IN AGE	PARENTS 40-49 IN AGE	PARENTS 50-59 IN AGE
Facebook	64%	66%	60%	51%
Instagram	37%	28%	18%	10%
Snapchat	33%	11%	5%	3%
Twitter	11%	8%	11%	9%
YouTube	43%	30%	23%	19%
Video msg	27%	23%	19%	17%

54

Tech Ethics

- Should schools and school psychologist have same policy regarding online interactions for everyone?
- Should the decision be made individually, depending on the function for that particular student or parent?



55



Ethics Code and Social Media

Preamble

- Professional vs personal behavior
 - Blurring of boundaries
 - Social media
- School psychologists held to higher standard of good character and conduct as they serve as role models for children.



56



Privacy and Confidentiality
Std. I.2.3

- Social Media and Personal Identifiable Information (PII)
- In online discussion groups
 - Do not disclose PII so client can be identified

57



Said No School Psychologist Ever

- Common ethical issues
 - Oversharing and too much detail in posts
 - People wanting to do detailed case consults
 - What's funniest person's name
 - What's funniest response to specific items on tests



58



Said No School Psychologist Ever

- Common ethical issues
 - Screenshots to get people in trouble at work.
 - Too judgmental regarding parents or teachers
 - Engaging in unprofessional behavior and name calling.



59



Social Media Standards

- [Standard III.5.1 Private Versus Professional Conduct](#)
- [Standard III.5.2 Separation of Personal Beliefs](#)
- [Standard III.5.3 Personal Beliefs and Experiences](#)
- [Standard III.4.3 Harassment and Exploitation](#)
- [Standard IV.2.4 Participation in Public Discourse](#)

60



Scenario Interested Dad

- Single father with two daughters
 - Daughters have anxiety and behavior disorders
 - E-mails school staff constantly accusing them of wrongdoing.
 - Makes presumptuous demands
 - Demeaning insults of staff
 - Face to face – interactions that are aggressive, hostile and intimidating.

61



Court Case

- LF v. Lake Washington No. 414 School District
 - School put parent under communication plan
 - No response to e-mail or any other form of communication other than bi-weekly meetings.
 - Parents violated and meetings moved to monthly.
 - Court sided with school
 - Ruled plan did not restrict parent’s speech but merely regulated types of communication district responds to.

62

E-mailing Students and Families

- Situations
 - Counseling relationship
 - Assessment procedures
 - Counseling vs. administrative e-mails
 - Checking e-mail
- General rule
 - E-mail communication must support the working alliance between school psychologist, student and family to promote trust



63

E-mail Confidentiality and Privacy

- Must list
 - Acknowledge e-mail is not confidential
 - Ensure e-mail platform is encrypted and password protected
 - Determine what information will be ok to disclose in e-mail
 - Acknowledge one will never forward student or family e-mail
 - Determine policy for recording e-mail in student record/have school policy
 - Ask student and family about privacy of their e-mail accounts and who has access

64

E-mail

- Typically least protected for student confidentiality
- HIPAA Best Practice Recommendations (Oliver, Oct 2013):
 - Use only sanctioned email providers
 - Email to only one recipient at a time
 - Notify parents prior to using email
 - Recommend parent provide personal over work email
 - Verify recipient email address prior to sending
 - Include “Unintended Recipient Directions”
 - Limit confidential info to attachments only
 - Utilize password protection on documents
 - Tag email communities as “Confidential”
 - Utilize “Expiration” feature (5 days)
 - Mask personal identifiable information



65

E-mail



- Sample disclaimer language
- **Confidentiality Warning:** *This e-mail contains information intended only for the use of the individual or entity named above. If the reader of this e-mail is not the intended recipient or the employee or agent responsible for delivering it to the intended recipient, any dissemination, publication or copying of this e-mail is strictly prohibited. The sender does not accept any responsibility for any loss, disruption or damage to your data or computer system that may occur while using data contained in, or transmitted with, this e-mail. If you have received this e-mail in error, please immediately notify us by return e-mail. Thank you.*

66

Whither Texting?



- Many students and families prefer this mode due to ease of communication
- Similar issues regarding e-mail
- Short Message Service (SMS) is not encrypted, secure of HIPAA compliant

67

Texting



- Stop texting service information until policies are in place
- Encrypt all mobile devices
- Develop text usage policy
- Develop a “Statement of Understanding” for text-using students and families
- Explore secure text messaging solutions
 - Eg. Signal, TigerConnect, Wickr



wickr

68

Caution! BYOD is an Issue

- Do you bring own computer to work?
 - Called Bring your Own Device – BYOD; Smartphones too!
- Or do you use school’s computer for personal tasks, including email, social media, etc.?.
 - Have two accounts on computer – personal & professional
 - Use Administrator function to do this



69

Password Guidelines

- Don't be obvious
- Don't use existing online passwords
- Don't use a regular word
- Mix cases, number, and punctuation
- Change passwords regularly
- Don't share password or write down
- Create hierarchy of passwords
- Use two-factor authentication



70

Common Passwords



71

Which Password is Stronger?

- D0g.....
- PrXyc.N(n4k77#L!eVdAfp
- Hint: not the long one!!



72

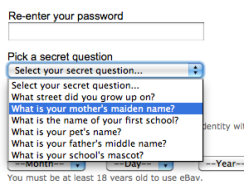
Passwords – Make it Strong

- Aquarius Time to Crack - 9.08 minutes
- Aquarius1 Time to Crack – 1.59 Days
- Aquar\$ius1 Time to Crack – 19.24 Years
- Aqu57ar\$iu3s Time to Crack – 17,400,000 Yrs
 - Caps/case do count too; have unique password for EACH account
- It is really easy!
- Some servers do not allow symbols; insert CAPS in middle or end
- Thieves will use your “forgot password” access
- Hacker software: 8 Billion password checks **per second**
- **Use all the numbers allowed = 14, or 8 or...**

73









Beyond Passwords – Security Question

- Another layer of protection
 - Misspell the street you grew up on or your first boy/girlfriend.
 - Use street name of your best friend and you know!
- Encryption
 - Necessary – likely
 - Best Practice
 - How?



74

Storing Passwords Free PC Magazine Recommends

 <p>LogMeOnce Password Management Suite Premium Best for Abundance of Password Management Features</p>	 <p>Symantec Norton Password Manager Best for Extra Web Protections</p>
 <p>Bitwarden Best for Open-Source Password Management</p>	 <p>Avira Password Manager Best for Simple Password Storage</p>
 <p>WWPass PassHub Best for Security-First Password Management</p>	 <p>Enpass Password Manager Best for Syncing Passwords Using Personal Cloud Storage</p>
 <p>NordPass Best for Managing Passwords on a Single Device</p>	 <p>KeePass 2.34 Best for DIY Password Management</p>

75

Keep Accounts Locked Down

- Hardware Security Keys
 - Insert key into USB port after entering password
- Titan Security Key
 - Phishing resistant two-factor authentication
 - Second lock after password
 - Uses FIDO2 protocol (encryption)
 - Good on Google, Facebook, Twitter
 - \$25-85 for key
- Others – Yubico & YubiKey



76

Storage of Records

- Differences among companies about how long the data can be stored and what information can be used by companies.
 - Pearson
 - Houghton Mifflin Riverside
 - PAR
 - MHS
 - Google Workplace for Education
- Look for privacy statements on websites



77

School Clouds and School Psychs

- School psychologist often mandated to use school cloud services for records.
 - **READ POLICIES or Make them**
- Many districts are violating FERPA issues regarding student information disclosure in general.
- What about protected populations being served?
- School psychologists are responsible for protecting their data.

78



Record Keeping Std. II.4.9

- School psychologists, in collaboration with administrators and other school staff, work to establish district policies that are consistent with law and sound professional practice regarding the storage and disposal of school psychological records.
- They advocate for school district policies and practices that
 - Safeguard the security of school psychological records while facilitating appropriate access to those records by parents and eligible students

79



Encrypting Documents

Keeping Information Safe and Confidential

80

Encryption – Is BETTER



- 128 bit is ok
- 256 bit security preferred
- Advanced Encryption Standard (AES)
 - Standard for U.S. Government
- HIPAA – not apply to schools – yet!
 - Personal Health Information (PHI)
 - Word processing files transmitted electronically
 - E-mail and texting between psychologist and school personnel, parents, and/or students.

81



Encryption

- Decide what needs to be encrypted
 - Folders and files with PII top priority
 - District policies on employee encryption
 - Check with district IT
- Encryption Program Types
 - Processing individual files and folders
 - Virtual Disk Drive



82



Google Workspace for Education

- Google does not own any data that institutions put into the Google Workspace for Education platform
- Google does not collect, scan or use data in Google Workspace services for advertising purposes
- Data can be deleted or exported by authorized users at any time

83



Google Workspace for Education

- Aligned with all compliance needs of K–12 education, including FERPA and the COPPA.
- Meets requirements of several other privacy pledges, data standards and assessments.



84

Keeping Google Docs Safe



- Keep Google account login secure
 - Use strong password
 - Enable two factor authentication
 - Possible use of hardware security key
- Encrypt documents before uploading
 - Can store but can't edit files on Google Docs
 - Encrypt with Word
 - Encrypt with Boxcrypt
 - Encrypt with Veracrypt

85

Protect Microsoft Word Content



- Microsoft Office 2013, 2016, and Microsoft 365
- Utilizes 128-bit encryption.
- Option for:
 - Read-only mode
 - Password protection
 - Editing restrictions
 - Digital signatures

86

How to Encrypt a Word Document



- Click on *File* tab and click on *Info* option.
- Screen will open and now *Protect a Document* box will be available.
- Clicking on *Protect a Document* box gives option to *Encrypt with Password*.
- Give a password for the document and verify it.
- Same process to de-encrypt except delete saved password

87

Encryption Options

- AxCrypt Premium
 - Secure files and folder
 - Secure files on cloud servers
- NordLocker
 - Creates encrypted storage lockers
 - Easy to use and integrates with Dropbox
- Folder Lock
 - Encrypts files or locks them
 - Allows shredding of files



88

How Encrypt for the Cloud

- BoxCryptor – all OS + Mobile
- Boxcryptor.com – free version available
 - Can link to cloud drives (only 1 for free version)
 - Put files into boxcryptor folder which is linked to cloud storage
 - Drag and drop files to encrypt and store.
 - Within boxcryptor, able to open and close like usual.

89

How Encrypt for the Cloud

- BoxCryptor – all OS + Mobile
 - If try to access outside program for cloud, access is denied.
 - Right click, *Show in BoxCryptor* and able to open.
 - Option to provide others access with e-mail address



90

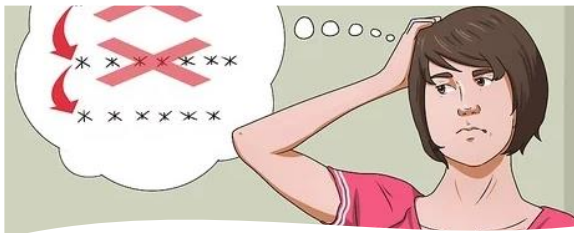


Other Encryption

- Cloud
 - Veracrypt
- Whole drive - Microsoft BitLocker
- USB Drives
 - Kanguru drives
 - SanDisk PrivateAccess
 - Complimentary encryption



91



Words of Warning

- Pick a good password
- Pick a way to remember passwords
 - Encrypted Excel or Word file
- Check with school district regarding encryption policy.
- Don't put password of encrypted document in same e-mail in which document is attached.

92

Cloud Storage Services



93



Assessment and Intervention

Std. II.3

- Principle applies to use technology such as computer-assisted and digital formats for assessment and interpretation, virtual reality assessment and intervention, distance assessment and telehealth intervention, or any other assessment or intervention modality.

94



Tech Ethics Questions to Ask

- Who owns the information?
- Where is the information being stored?
- How is the information being stored?
- How long is that information going to be stored?
- Who has access to the information?
- What safeguards are in place?

95



Tech Ethics Questions to Ask

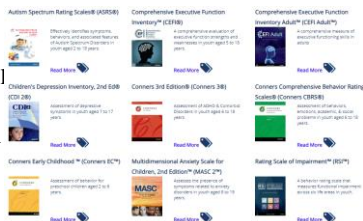
- Which has greater security capabilities?
- What are the vulnerabilities of the cloud?
- Is there incident detection/response?
- Look at security monitoring
 - How will you exercise control over data?
 - What are potential legal concerns?
 - Does it comply with FERPA?

96

Cloud Assessment Software



- MHS – rating scale cloud scoring and e-mail of rating scales
- FERPA & HIPAA compliant
- Recent website update



97



Cloud Assessment Software is Changing

- Multi-Health Systems
 - Three options to administer measurements
 - Administer in-person while online
 - Administer by sending person an e-mail link
 - Print the form for paper and pencil
- Automated scoring online
- Generates reports
 - Assessment/Interpretive
 - Progress
 - Comparative

98

Cloud Assessment

- PAR – iConnect – administer instruments, interpret results, and examine client assessment



99



- Saves time but not necessarily money
- Increased flexibility in administration and scoring (cross-battery not allowed)
- HIPAA Compliant
- Update – not store data on servers once instrument scored.
 - Information erased upon completion

100



Cloud Assessment

- **Pearson**
 - **Q Global** – includes most Pearson assessment
 - 60 measures available and more coming
 - Offers Digital Assessment Library for Schools
 - Unlimited online access to 40 instruments
 - Wechsler and Kaufman assessments
 - Q-global Video Proctoring
 - Telehealth assessments
 - No IQ or Achievement tests

101



- Saves time but not necessarily money
- Increased flexibility in administration and scoring (cross battery allowed)
- Practitioner owns the data
- Information stored on servers in Toronto and back-ups in Vancouver
- HIPAA and HITECH Compliant
- See their White Paper
 - Q-interactive Data Security & Privacy July 2015

102



Privacy and Confidentiality

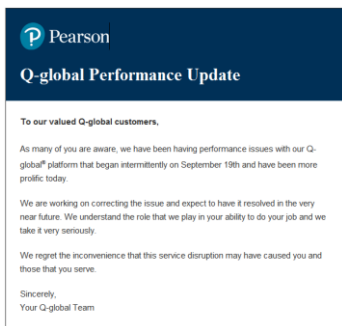
Std. I.2.1

- Minimize intrusions on privacy
- Do not disclose or store in education records any privileged information except as permitted by the mental health provider–client privilege laws in their state.
- Carefully consider whether to share 3rd parties information that could put others at risk.

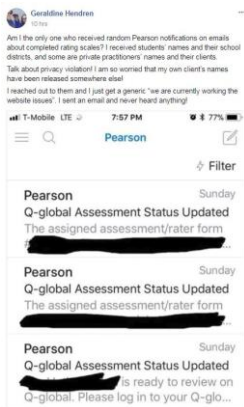
103

PEARSON

September 20, 2017



104



PEARSON

- Inadvertent disclosure
- Questions
 - School psych response
 - FERPA violation
 - Parent notification



105



Assessment and Intervention

Std. II.3.5

- When using digitally administered assessments (e.g., computers, tablets, virtual reality) and/or computer-assisted scoring or interpretation programs, school psychologists choose programs that meet professional standards for accuracy and validity.
- School psychologists use professional judgment in evaluating the accuracy of digitally assisted assessment findings for the examinee.

106



Changes from 2010-2020 Standards

- Acknowledgement of limit of knowledge over digitally scored instruments.
- 2010 - If using computer-assisted assessments, computer scoring and/or interpretation programs, they must be accurate and valid.
- 2020 – More flexibility in definition towards professional judgment.

107

Testing on iPad

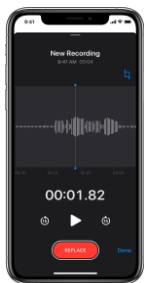


- Are results equivalent with paper and pencil compared to iPad?
 - Yes – Test behaviors of children are not negatively influenced by test format.
 - Neither internalizing or externalizing factors are impacted by format.

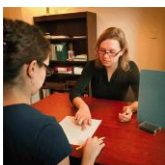
Castro, C.J., Vezzi, K., Dumont, R. & Guiney, M. (2019). Exploration of children's test behavior during iPad administered intelligence testing. *Journal of Psychoeducational Assessment*, 37, 3-13.

108

Scenario – Let Me Get That Down



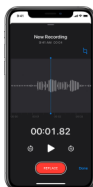
- Student brings phone into testing session.
- School psychologist finds that student has been recording session.
- What is to be done?



109

Scenario - Issues

- Test security – federal copyright protection
 - Violation when any test materials are audio or video recorded.
- State law
 - Party requirement to agree being audio recorded.
- Follow-up with parent or student to address underlying reasons for recording



110

Protecting Student Data

- Steps for school employees to follow:
 - Check with your IT department before using apps or software.
 - Don't keep or share student data any more than you have to.
 - Don't share personally identifiable information about students in email.
 - Don't use actual student data for training purposes.
 - Keep your devices secure.

111

Cloud Computing and Schools

- Most school districts have in-house servers restricted to use only in district
- States have embraced state-wide cloud systems
 - 95% of districts rely on cloud services for data mining related to student performance, support for classroom activities, student guidance, data hosting, and special services like cafeteria payments and transportation planning



112

FERPA and the Cloud

- Contractually identify cloud vendor as a “school official” under “direct control” of the education institution
- Five principles for schools to follow:
 - Maintain control of student data
 - Expressly prohibit the mining of student data for advertising and marketing purposes
 - Enter into a comprehensive agreement covering all of the cloud services provided to the education institution
 - Consider how providers may use anonymized data
 - Conduct due diligence into the cloud service provider’s practices with respect to student data

113

COPPA Issues

- Information on children under 13 do the following:
 - Provide parental notice of their information practices
 - Obtain prior parental consent for collection, use, and/or disclosure of personal information from children
 - Empower parents, upon request, to review the personal information from their children
 - Provide a parent with the opportunity to prevent further use of personal information that has already been collected or the future collection of personal information from that child
 - Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information
- To the extent that data analytics services collect information directly from school children or enable the tracking of school children based on their interactions with the cloud service, COPPA obligations would apply

114



and yet....



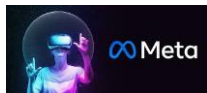
- 25% of districts inform parents of their use of cloud services
- 20% of districts fail to have policies governing the use of online services
- 25% of the agreements specify the purpose for disclosures of student information, fewer than 7% of contracts restrict the sale or marketing of student information by vendors, many allow vendors to change the terms without notice
- The majority of cloud service contracts do not address parental notice, consent, or access to student information
- School district cloud service agreements generally do not provide for data security and even allow vendors to retain student information in perpetuity with alarming frequency

Source: Fordham Law Center (2013)

115

Looking Forward

- AI Bill of Rights
– proposed by Biden administration
- Virtual reality assessment
- Data privacy in the Metaverse



116

Contact the Presenter

- Dan Florell, Ph.D. , NCSP
- Eastern Kentucky University
– Dan.florell@eku.edu
– Twitter: @schoolpsychtech
– Facebook: “Like” MindPsi



117
