OPRE

Research-to-Practice Brief

THE USE OF TECHNOLOGY TO SUPPORT EARLY CHILDHOOD PRACTICE: PROTECTING CHILD, PARENT, AND PRACTITIONER PRIVACY

OPRE Report 2016-18
February 2016

Over the past two decades, the use of technology in early childhood settings has steadily increased, growing out of the recognition that technology may be used to improve program practice and, ultimately, children's learning and development. The Administration for Children and Families (ACF) Office of Planning, Research and Evaluation (OPRE) recently contracted with NORC at the University of Chicago to review the knowledge base related to the uses of technology to support early childhood practitioners who work directly with children and families. A description of the project and links to the report and three research-to-practice briefs may be accessed at the following webpage: Use of Technology to Support Head Start Practice, 2013-2015.

This brief, intended to complement the review, addresses privacy and security considerations related to computer software, mobile applications (apps), and web-based tools that early childhood practitioners may access via the Internet as part of their work with children and families. Examples include online packages that capture child assessment data and instantaneously provide teachers with data-based instructional suggestions; programs that use live video conferencing to connect parents and home visitors; and remote coaching models in which teachers use an online submission process to share video recordings of their own practice. As with the review of the knowledge base, the focus of this brief is technologies that support early childhood practice, rather than technologies intended for independent child use or technologies that require little or no direct practitioner involvement. Drawing on guidance developed by the U.S. Department of Education's Privacy Technical Assistance Center (PTAC), this brief provides a set of best practices to guide early childhood programs in strengthening the safeguards to protect child, parent, and practitioner information as programs increasingly incorporate technology to improve practice.

This brief presents some best practices that can guide early childhood programs in evaluating the use of online services to support practitioners in their work with children and families.

WHAT IS A REAL-LIFE EXAMPLE OF APPLYING PRIVACY AND SECURITY CONSIDERATIONS IN AN EARLY CHILDHOOD SETTING?

As the director of an early childhood program, you have noticed that your teachers seem to be struggling with managing and aggregating child assessment data and applying it to instruction. You have found an online package that could help with this. It collects child assessment data directly via desktop or mobile access, scores the data, and produces reports that summarize how each child is progressing and provide suggestions for individualized instruction.

WHAT INFORMATION MIGHT COMPANIES THAT PROVIDE TECHNOLOGY TOOLS TO EARLY CHILDHOOD PRACTITIONERS COLLECT?

What types of information do we need to think about companies collecting? When you are utilizing a service that takes advantage of online capabilities, it can sometimes be easy to forget that personal, sometimes identifying information, is being collected. There are different levels of this kind of data, from the most sensitive and personal to the broadest, most meta-level data. For example, at the most personal level is information that can be used to distinguish or trace an individual's identity. If a teacher is using an online package to produce suggestions for services and instruction tailored for individual children, accounts must be set up for each child, using names or identification numbers, so that developmental data, such as assessments, may be linked to individual children. On a less personal level, companies can collect information that is aggregated and is not linked or linkable to specific individuals, such as classroom-level data. An example of this would be data collected as children or teachers interact with an online program but do not log in to individual accounts. Finally, companies may collect what is known as "metadata," defined as the contextual or transactional information surrounding other data that are collected. Examples of metadata that might be gathered include the number of times a student attempted a question or the length of time taken on an activity. Metadata may or may not be stripped of identifying information.

Companies that provide technology tools via the Internet may collect a variety of information. Early childhood programs play a critical role in protecting child, parent, and practitioner privacy.

HOW CAN PROGRAMS PROTECT THE PRIVACY OF CHILDREN, PARENTS, AND PRACTITIONERS?

To make sure that any service you use protects the privacy of children, parents, and practitioners, consider the following questions:

- Are you familiar with applicable privacy laws? Does this new software comply with the laws? Laws to consider include:
    - Children's Online Privacy and Protection Act (COPPA)
    - Family Educational Rights and Privacy Act (FERPA)
    - Protection of Pupil Rights Amendment (PPRA)
    - Children's Internet Protection Act (CIPA)
    - Any relevant State laws
- Have you considered all of the online services or packages currently used in your program? Do you have a complete list of everything being used?
- Do you have an approval process for the use of online services (including free services) by teachers and others who work with families?
- Do you have a written contract or legal agreement with technology providers that you can use whenever possible?
- Is the product used by your larger school district, program, or community? If the consumer products are not purchased through the school, are you exercising additional caution?
- Are you being transparent with parents and communicating with them openly about questions of privacy? Are you considering which technologies and circumstances may warrant parent approval?

It is important to establish policies and procedures that protect the privacy of children, parents, and practitioners. These should include the evaluation and approval of written and click-wrap agreements as a method to protect the personal and meta-data collected by the technology provider. The following are considerations related to these methods.

See this list of questions to make sure that any service you use protects the privacy of children, parents, and practitioners.

WHAT SHOULD BE INCLUDED IN A WRITTEN AGREEMENT OR CONTRACT?

- **Security and Data Ownership Provisions.** Consider whether the data being collected belongs to the program or to the company providing the online service and be sure this is clear in the contract. Have you outlined each party's responsibilities in the event of a data breach? Have you established minimum requirements for security controls? You can also consider allowing for a security audit to make sure the data your center is collecting is as secure as possible.
- **Data Use, Retention, Disclosure, and Destruction Provisions.** Have you considered how the company providing the online service can use the information collected? Be sure to define the specific purposes for which the company can use this information, as well as specifying with whom the provider may share information. In order to be careful about what happens after the contract period is expired, include data archival and destruction requirements. When appropriate, you can also define procedures the company will carry out to avoid disclosure.

- **Collection Provisions.** As teachers are collecting information from assessments, very specific data is being collected. In your contract or agreement be sure to think through this data and be specific about the information the company will collect (e.g., forms, logs, address, name).
- **Data Access Provisions.** Once data is available online, it can theoretically be accessed by parents, teachers, and anyone else with interest in your program's data. Have you carefully specified which program staff and/or parents will be permitted to access specific data? What is the internal process for obtaining information?
- **Modification, Duration, and Termination Provisions.** What is the length of your agreement, and what are the procedures for modifying the terms of the agreement (mutual consent to any changes is a best practice)? If you no longer want to use this service, what are the responsibilities of both your program and the service provider upon termination of the agreement?
- **Indemnification and Warranty Provisions.** Finally, what will you require the service provider to do to comply with applicable state and federal laws, and what does the service provider agree to do to remedy a violation of these requirements (e.g., compensate for damages resulting from the provider's violation)?

WHAT EXTRA STEPS ARE NECESSARY WHEN ACCEPTING CLICK-WRAP LICENSES FOR CONSUMER APPS?

Programs sometimes can't negotiate agreements with providers of consumer apps, and are faced with a choice to accept the providers' terms of service (TOS) or not use the app. In this case, Click-Wrap agreements typically come into play. Click-Wrap agreements ask users to agree to specific, terms and conditions. Users typically click a box that says "OK,", "I Accept", or "I Agree" in order to use the product. If you reject the agreement, then you cannot use the product or service. Click-Wrap agreements are often included with installation or entry into an application and may contain the necessary components to be considered legally binding. Even though the terms are already written, there are still steps you can take when using Click-Wrap consumer apps:

- **Check Amendment Provisions.** Be sure to carefully review the TOS. Has the company retained the right to amend the TOS without notice? If so, are you comfortable with that? And remember that, if the TOS can change, it is necessary to review these agreements regularly to determine if any provisions have changed, and if so, re-evaluate whether to continue using the service.

- **Print or Save the TOS.** When accepting a Click-Wrap agreement, print or save a copy of the TOS that you have agreed to.
- **Limit Authority to Accept TOS.** As the director of the program, do you feel comfortable with all of your staff members accepting Click-Wrap agreements? Click-Wrap agreements can be easily accepted, without going through approval channels. Individual staff members may not understand the specifics of how the provider will use and secure data. Programs should develop policies outlining when individual staff members may download and use Click-Wrap software.

Remember that Click-Wrap agreements can impose terms and conditions that affect the privacy of the practitioners, children, and families who use the service. Carefully consider what is exchanged for the use of the app. Pay particular attention to the information that the service provider will collect, what the provider will do with the information, and whether you must give up the right to sue for damages caused by using the service.

****

Technology can be a great asset to early childhood programs. These privacy and security considerations can help ensure that technology is used in the safest and most appropriate way possible.

OPRE Report 2016-18
February 2016

Authors:

Kathleen Dwyer, Sonja Hatten, and Elisa Rosman

Office of Planning, Research and Evaluation; Administration for Children and Families;

Department of Health and Human Services

www.acf.hhs.gov/opre

Suggested citation:

Dwyer, K. M., Hatten, S., & Rosman, E. (2016). *The use of technology to support early childhood practice: Protecting child, parent, and practitioner privacy.* OPRE Report 2016-18. Washington, DC: Office of Planning, Research and Evaluation, Administration for Children and Families, U.S. Department of Health and Human Services.