

Snap! privacy guidance for teachers and school districts

See also our *privacy policy*, snap.berkeley.edu/privacy.

Recent legislation in many parts of the world has led school districts to ask suppliers of computing services to sign privacy agreements making certain guarantees about how student Personally Identifiable Information (PII) is collected, stored, and used. In the United States, we get many such requests from schools using the *Beauty and Joy of Computing* CS Principles curriculum and from schools using the TEALS Introduction to Computer Science curriculum.

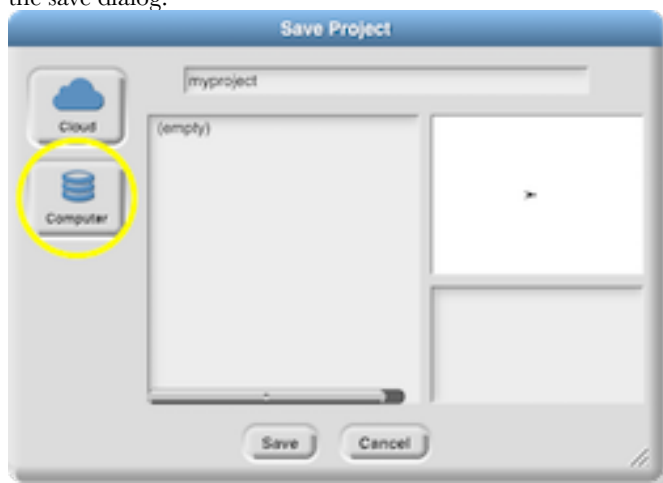
For reasons explained below, we can't sign your privacy agreement, but we are very committed to privacy, especially for children, and you can rely on that. Here are the main points to understand:

1. **Snap! and the Snap! Cloud are two different things. You can use Snap! without sending us *any* information, PII or otherwise.** We don't have to know you exist. To use Snap! in this way, you save programming projects on your own computer, rather than in our cloud storage. This is the *best practice* for maintaining legal compliance; we recommend it to schools.

To use Snap! in this way, you connect to our web site as usual: snap.berkeley.edu/run. This will download Snap! to your browser, and you have no further need to interact with us in that session.

We do log IP addresses of clients, so we could possibly determine that *someone at your school* has used Snap!. But we wouldn't know who; IP addresses alone are not generally considered PII. If even that bothers your lawyers, you can set up your own Snap! server by downloading our GitHub repository: github.com/jmoenig/Snap/releases/latest. If you do this, your IT person should check regularly for updates, which are announced on our forum, on the BJC Teachers forum on Piazza, and on the TEALS forum.

Once you have Snap! running in your browser, when you want to save a project, select "Computer" from the save dialog:



The project will be saved in the browser's download location.

2. Even if you use the Snap! cloud to store your projects, we collect only one piece of what *might* be considered PII: an email address to be used for password reset requests. The *best practice* for schools that want to use the Snap! Cloud is to set up class accounts in bulk, separate from any personal Snap! account a student might have, and use *the teacher's email address* for all of them. Then we unambiguously collect no student PII.

Apart from the question of PII, there are other practical reasons for using the teacher's address: It allows the teacher to handle lost passwords on the spot, without having to work out which email a student might have used. And it means the accounts are ready to go on the first day of class, without wasting that day getting everyone set up.

"Collect" means that *we ask for* a piece of information. Section 5, below, discusses how students might *choose* to put personal information *in a project*. We can't police that.

It's important not to undo the anonymity of your student accounts by, for example, using the school's student ID number as the Snap! username. Student ID numbers are definitely considered PII; we don't want to know them.

Our lawyer thinks that a student email address *by itself* is not PII. But we prefer a solution that doesn't depend on your lawyer having the same opinion as ours. We need an email address; if it isn't the student's, that simplifies everyone's life.

3. We're good guys. We do not profit from offering Snap!, neither directly via user fees nor indirectly through advertising or other creepy practices. No third parties have access to users' email addresses, the only potential PII we collect. We do not profile users, period. We were already paranoid about Facebook and Google back when everyone thought those companies were your friends. Please don't let a rigid rule designed for commercial for-profit providers of computing services get in the way of letting your students use Snap!.

4. But we can't sign a contract with you. There are three reasons:

(1) *Legally, there is no contract without mutual consideration.* That means we promise to do something for you, and you promise to do something for us. (In a typical commercial contract, the latter would be your promise to pay the company money.) But with Snap!, you aren't doing anything for us. We don't charge money. We don't benefit in any way from your use of Snap! other than feeling proud of our work.

(2) *We are not authorized to sign contracts* on behalf of the University of California, Berkeley, which is the organization that sponsors our work. And the University's lawyers would never agree to a contract that exposes the University to substantial risk (if, say, someone breaks into our computer and steals our users' email addresses and you sue us) for no benefit.

(3) *Those boilerplate contracts typically require us to provide services* that we are not equipped to provide, such as audits, daily backups, and/or interfacing with your classroom management system. We are half a dozen developers, with no IT staff and zero budget. *Commercial* providers of computing services to schools factor the cost of services like these into the fees they charge you.

If you follow one of the best practices recommended above, you don't *need* a contract with us, because we collect no student PII.

Beyond those main points, there are two other things you should understand about the nature of the service we provide and the ways that kids use it:

5. **We have no control over what *unsolicited* information you or your students send us.** This means that we might *possess* PII that we don't *collect*, without knowing we have it, so we can't promise that there is no PII stored in our cloud storage. For example, if a child makes a Snap! project that says "I'm 15 years old today" (as happens frequently in Scratch) that's a piece of PII that is in our cloud, but we don't *know* we have it. We can't teach your students to protect their privacy. We do encourage them to be careful, in our official privacy policy, but children are children. Similarly, we have no control over choices *you*, as a teacher or administrator, make. If you create accounts for your students that use your student ID numbers as the usernames, you are giving us PII that *we do not want* and can't control. Usernames, in particular, are visible to anyone who uses our community web site.

6. **Our users *want* to share information with each other.** This is another reason why you should set up the accounts for class use yourself, separate from students' personal accounts. We have a community web site, snap.berkeley.edu, where users can publish their programming projects and comment on each others' work. They learn from each other and from us (we participate on the community forum at forum.snap.berkeley.edu). We may also aggregate information from *published* projects for research purposes. So if you do choose to use our cloud storage, you should disallow publication of projects from class accounts. You are then not responsible for what someone who happens to be your student does outside of school on their separate personal account.