Digital platforms for communication and information sharing

Digital technologies in education are now common and expected. When our tamariki are such confident users of ICT, educators, parents and whanau need to match that digital fluency. It makes sense that as communication has changed with instant messaging and social media, ways of sharing learning and school information have changed too.

There are number of software applications (apps) such as Seesaw, School Stream and Hapara that the education sector has embraced to share information. These are promoted as being platforms for student engagement, where children can express themselves and their school work. Parents can see and hear what their children are learning, thereby understanding development and engage meaningfully. Teachers and administrators can collect information digitally and not have stacks of hard copy documents and forms, and absentees and school notices can be easily shared.

There certainly are positives in strong family and community engagement. Children will feel ownership in their work and take pride in sharing with whanau. With the download of an app, or accessing a website, parents can have real-time access to information, and particularly after events such as the earthquakes will have a communication channel.

But before diving in, there are some privacy points everyone needs to think about. Personal information is just that, personal, and it can be embarrassing or there may be unintended consequences from sharing and using information. A picture that seemed okay to share at the time may feel different in the future. Consider how might your child feel about shared content once they are older and how it might affect them. We need to think about the future, and what could happen to all the data that is collected over our children’s lives

Privacy points

- What kind of information is collected?
- Who can access the information?
- Where the information is kept and for how long?
- How is, and how could the information be used?
- What are the terms and conditions of the app/software?

Knowing and understanding the technology is part of digital citizenship. Putting some thought into these points will ensure that schools, caregivers and children are respectful of privacy and the right to privacy is protected.

Questions for **parents** can include:

Question	**Why should I ask?**
What information is being collected?	Aside from the app having your children's work and photo, what other information do you have to hand over? Bear in mind that hidden in the fine print of an app may be the ability for the app to collect details of your Google/Facebook account, your IP address, your mobile carrier and your location – which quickly builds up a picture of you.
What information is being shared?	You might be fine with your child's photo being posted in the app or might prefer photos taken from behind. Do you want all other parents to see things? What is your preference/level of comfort? You can then make an informed choice.
Are there any options around the content being posted?	Can only certain content be posted? If you did not want photos of your child's face posted, how is that going to be managed?
Are you clear on the purpose and use of the app?	It's obvious that you want to see your child's information, but what else might the app be used for other than to see learning? Will this be used for grading/reporting or a behaviour tool?
Do your whanau know how to share safely and responsibly?	What are the school's, and your child's expectations for your involvement? This will ensure consent and respect. What kind of comments might be shared in the app? It might be very easy for private/identifying details to be become available if someone tagged a photo of your child that had detailed comments. (e.g. their full name and something about their family).
Where else might the information go?	Is the information in the app being shared with other social media platforms or your email provider?

Questions for **schools** can include:

Question	**Why should I ask?**
Do you know the functionality of the app you are signing up for?	Doing your due diligence will ensure you understand all the potential risks and privacy implications and can then consider mitigations. It also ensures you are providing the best product/service to your community – you are aligned with your purpose(s) for using the app and collecting information.
Have you seen terms and conditions and the privacy policy?	Knowing and understanding privacy provisions in the fine print and privacy policy is just best privacy practice. Though it may be in legalese, you should understand how data is used by the provider of the app, for example third party advertisers, and how data will be kept safe. Ask questions, so that you are then not committed to something you don't understand privacy wise or don't want.
Who are you contracting with?	You then know who you might have recourse to if things were to go wrong, like in the event of a data breach.
Is the entity/app owner based overseas and where is your data stored?	You may have greater control and recourse if you have specified that the information and data be stored here in New Zealand.
What is the set-up of accounts?	Ensuring you have a good system for how users set up their accounts and ideally discouraging the practice of sharing account log in details means that there should not be risks around unauthorised access or sharing.
How will accounts be managed and deleted?	People are entitled to have their information removed if there is no longer a purpose for holding it.
What is your policy and process for content in the app?	Everyone needs to understand what appropriate content is. Having things clearly documented means that there is clear structure and expectations for content. Having a policy here links into your other school policies, such as good conduct and data use.
What communication have you provided to parents/caregivers?	Making parents aware what the technology is and how it will be used and providing adequate time to consider this means an informed choice can be made.
What opt out options are there?	Parents should be given a clear opt out, or a meaningful and appropriate way to manage any privacy concerns they may have.
What training have you given to your Kaiako/people?	Staff will then be empowered to have the right conversations with parents and can directly manage privacy concerns.

Many of these questions can be covered off in a Privacy Impact Assessment (PIA). This is a tool to identify and assess privacy risks and opportunities around collection, use and handling of personal information.

It does not need to be completed by a lawyer, though it may be useful to have legal input. Your Privacy Officer can work with the relevant people to prepare the assessment. It's important that the right people are included and that you have good conversations with your Digital/ICT teams – they can help with security requirements.

Start the PIA early on and before the app starts being used. A PIA does not need to be a long, complicated document, and importantly it is not static. You can revisit it over time and check back in on how you are meeting privacy expectations and best practice.

Resources

The Information Privacy Principles – link to New Zealand legislation online

Digital Technology safe and responsible use in schools – link to Ministry of Education PDF document

Office of the Privacy Commissioner’s Privacy Impact Assessment Toolkit – link to website

Netsafe kit for educators and schools – link to website