Managing privacy responsibilities in ECE

Introduction

In Term 1, 2015, ERO evaluated how well 200 early childhood services managed their responsibilities under the Privacy Act 1993. The evaluation looked at what service leaders knew and understood about their responsibilities around the collection, storage, use, sharing and disposal of information about children.

The use of new technology (such as the Early Learning Information system and online learning portfolios) makes it timely to look at how services consider the privacy principles when working with the range of ways information can be collected, stored and shared.

ERO was interested in how services managed privacy with both digital and paper-based information.

Privacy responsibilities

All agencies[1] must comply with the Privacy Act 1993. The Act controls how agencies collect, use, share, store and give access to personal information.[2] It also states that all agencies must have a privacy officer. The privacy officer is responsible for all privacy matters in the agency.

The Privacy Commissioner has developed a set of 12 privacy principles that provide guidance on how to meet these responsibilities. The Education Council Code of Ethics for Certificated Teachers also sets out some expectations for working with personal information.

The Code says that registered teachers must work to protect the confidentiality of any information about learners, in line with legal requirements; and that teachers will respect parents/guardians rights to access information about their children, except if it is not in the child's best interests.[3]

What ERO found

Most services in this evaluation were managing their privacy responsibilities well or very well. However, ERO's focus on privacy led to nearly half of the services improving their practices. Minor compliance issues were easily fixed, meaning that by the end of their review they were compliant. This finding suggests that services not in the sample should review their privacy practices.

In about a quarter of services staff were not in a strong position to ensure they met their responsibilities around the privacy of children's information. They did not have explicit

[1] An agency is any person or group, in either the public or private sector (with some specific exclusions, such as the Governor-General, or a commission of inquiry). Privacy Act, No. 28. (1993). Retrieved from http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html (21 September 2015).

[2] Personal information is information about an identifiable person. This means any information that can be traced to being about a particular individual. It may have their name, but sometimes information without a name will still have enough detail to be clearly about a particular person. Dalziel, K. (2009). Privacy in schools: A guide to the Privacy Act for principals, teachers and boards of trustees. *Office of the Privacy Commissioner.* Wellington. Retrieved from http://www.privacy.org.nz/assets/ (21 September 2015).

[3] Education Council of Aotearoa New Zealand. (2015). *The Education Council Code of Ethics for Certificated Teachers*. Retrieved from http://www.educationcouncil.org.nz/content/code-of-ethics-certificated-teachers-0.

knowledge of the privacy principles, and leaders had not provided clear, up-to-date policies to guide their practice. Most had not encountered any major privacy issues, but they did not have the knowledge or guidance to support them to act appropriately to minimise risk.

Understanding of the privacy principles

Most services had some staff that knew about their responsibilities around collecting, storing, using, sharing and disposing of information about children. This knowledge was not shared across all staff in some services.

Leaders in some services could state the privacy principles or their service's privacy policy, but did not understand what this meant for their practice.

The privacy principles are:

1. Only collect the information you need.
2. Where possible, get the information directly from the person.
3. Be clear about what the information will be used for.
4. Use fair and reasonable ways of collecting information.
5. Keep information safe.
6. Let people access information about themselves.
7. Correct information if the person thinks it is wrong.
8. Make sure information is accurate before you use it.
9. Only keep information as long as you need it.
10. Only use the information for the purpose you collected it.
11. Only share personal information if you have a good reason.
12. Only use identifiers if it is clearly allowed.

Privacy Commission (2014). *Privacy Principles Poster.* Retrieved from http://eli.education.govt.nz/eli-privacy/privacy-principles-poster/ (22 September 2015)

Where service staff were managing children's privacy well a range of methods were used to make sure they knew what to do. Induction processes, workshops, discussion of practices and risks at staff meetings, staff handbooks, and passing on notices from government agencies were all used to keep staff up-to-date with their responsibilities. Some services also discussed the implications for their practice when they were reviewing policies and procedures.

In home-based services, visiting teachers gave advice to educators about what information could be recorded and shared, how to store information safely, and what could not be stored, displayed or shared.

In some Playcentres, parents felt that privacy responsibilities did not apply to their context and information about all the children was available to all the parents.

Informing parents

Parents were informed about privacy matters through enrolment, induction packs and meetings. Playcentre training for parents also covered privacy responsibilities.

Services gave parents guidance around protecting other children's privacy, for example, reminding them to only take photos of their own child during sessions, birthday celebrations and trips.

Some services noted that it was a challenge to monitor parents' use of mobile phones for taking photos. They relied on trusting the parents to do the right thing.

Privacy policies

Where privacy responsibilities were managed well, services had a privacy policy and procedures to guide staff about how to collect, store, share and dispose of information. Comprehensive privacy policies covered the collection, storage, use, disclosure and disposal of information. They guided staff in:

- thinking about the reason for gathering information before collecting it, and informing parents about how the information would be used
- ensuring records were up to date (especially around custody matters and who was approved to collect the child) and supporting parents or guardians to correct personal information
- storing and disposing of records appropriately
- dealing with requests for information and sharing information with external agencies
- dealing with complaints about breaches of privacy
- Identifying privacy risks and ways to minimise risk.

In these early childhood services, other service policies (such as child protection and cyber policies) were also consistent with the Privacy Act and principles.

Some Playcentres were not aware of changes in membership, and new members were not always informed of the Association's privacy policy and what that meant for them. Policies were not always updated to reflect changes in membership.

Actions for maintaining privacy of children's information

Most services were keeping physical records of children's information secure. Management of physical records was more commonly an issue than management of digital records.

Digital records

Most services were using the Early Learning Information (ELI) system or an alternative. The system was often accessed only by the association or umbrella organisation, rather than individual services. All staff entering data were familiar with the ELI privacy guidelines.

In most services, passwords to service computers were only given to those who needed them, and were not shared. Staff were regularly reminded about not recording or sharing passwords. In a few services, there was no password protection on centre computers or many people knew the password.

Online tools were used in some services to electronically store and share children's assessment between educators and parents/whānau. In a few services, parent permission forms[4] had not yet been updated to recognise use of online portfolios.

Service leaders had developed policies and guidelines for how social media would be used. They consulted with parents before starting to use social media. Photos were not normally used on social media pages, and service leaders monitored what was being posted.

Parents were required to sign a parental consent form before services published children's work, photographs or videos online. Some services had a system where each photo was checked with parents before uploading. A few services were still developing their understandings about privacy and its implications for their practices involving the use of digital photos.

[4] Parents provided written permission for the taking and use of photos. In the best services, there was a tiered approach to parental permission, giving parents the opportunity to give permission for photos to be taken for different purposes (e.g. for their child's learning record; for display in the service; for advertising and promotion of the service).

Physical records

In the services managing privacy well, policies were clear about how long different types of information should be kept before being destroyed. Clear processes were in place for disposing of information safely. For example, hard copy information was burnt, or shredded by the privacy officer or a secure document destruction company.

Services that were not keeping physical records securely stored files on open shelves or in unlocked cabinets. Some cabinets were kept locked, but the key was clearly visible. In some cases, daily medication or accident records showed several children on the same page. Parents were able to see information about other children when reading about their own child.

In a few services, policies did not provide guidance about records disposal. They did not know how they should dispose of print records and had kept them all.

Privacy officers

Most services had a privacy officer. Many of the services that were part of a kindergarten or Playcentre association or part of a larger organisation met their obligations by having one privacy officer responsible for privacy matters across the association or organisation.

A central privacy officer is acceptable where there is a clear process for other staff to contact the privacy officer and where all other staff have had basic training in privacy law[5].

ERO found that in some services with an association or organisation level privacy officer, staff did not know who the privacy officer was; or when, why or how to contact them. Staff members in these services generally had a poor awareness overall of the privacy principles.

Role of the privacy officer

Privacy officers encouraged compliance with the Privacy Act by developing policies and procedures, providing training for staff, and supporting other staff. They acted as a reference point when teachers needed advice on privacy matters and worked with the Privacy Commissioner when complaints were investigated.

Where privacy officers were doing well, they actively monitored whether policies and procedures were followed. They were well supported with training in privacy matters and clearly documented responsibilities.

Some privacy officers had been appointed recently and had not yet received training in their role. Some had received support and advice from national or employer organisations, but were still learning about their responsibilities.

In a few services, there was not a clear privacy officer but someone, such as an administration officer or head teacher, said they assumed they were also the privacy officer.

[5] Ministry of Education (2015). *Early learning quality update- April 2015.* Retrieved from http://www.education.govt.nz/news/early-learning-quality-update-april-2015/ (24 September 2015).

Knowing what to do when parents/guardians are separated

While clear procedures guided service staff with what to do if non-custodial parents tried to collect children, staff at many services were unsure of how and what information to share with a non-custodial parent.

Many did not know about the guidance from the Ministry of Education around this.[6]

Monitoring and reviewing privacy practices

Many services did not monitor whether their practices aligned with the privacy principles or Privacy Act, or with their own guidelines. They could not be sure they were doing what they needed to do, and sometimes their practices did not reflect their policies.

Some services had a regular cycle of reviewing their privacy procedures, while others had done this because privacy was the focus of ERO's review. Some services consulted parents as part of the review process. Many had not reviewed their privacy policies or procedures in several years.

Review processes did not always include a regular review of what permissions had been given by parents, or allow parents an opportunity to change these if they wanted.

Conclusion

Clear, regularly reviewed privacy policies were key to supporting staff to know and meet their privacy responsibilities. While most services had some staff who knew about privacy responsibilities, services would benefit from making sure that all staff knew what they had to do to keep children's information private.

In general, service staff took their privacy responsibilities seriously. They were especially careful when it came to protecting children's privacy in a digital environment. Passwords were only given to those who needed them and were not shared between staff. Staff who used digital records were familiar with the privacy guidelines for the programme they were using.

Most services had a privacy officer, either at service or association/umbrella organisation level. Staff needed to know who the privacy officer was for their service, and how and when they should contact the privacy officer. This was especially important when the privacy officer was not on site.

Privacy officers supported staff to know how to act in accordance with the privacy principles and service policies. The next step for privacy officers is to regularly monitor whether staff practice aligns with stated intentions, and to ensure that privacy policies continue to be relevant to the technology used.

---

[6] Ministry of Education. *Professional Practice Regarding Separated Parents/Guardians.* Retrieved from http://www.education.govt.nz/assets/Documents/Early-Childhood/Licensing-criteria/Centre-based-ECE-services/GMA4ProfessionalPracticeRegardingSeparatedParents.pdf (1 October 2015).

Keeping up-to-date with the privacy principles is vital to ensuring staff meet their obligations for managing information about children.

Recommendations

ERO recommends that services:

- review their privacy policies and ensure the agreed practices are understood by all staff and are implemented in practice
- ensure staff know who the privacy officer is and what their role is
- use this resource and the links provided to find out more about their privacy responsibilities.

Find out more

The Early Learning Information System- Information and privacy

Ministry of Education. *Information and Privacy.* http://eli.education.govt.nz/questions-and-answers/information-and-privacy/#58

The privacy principles

Privacy Commission (2014). *Privacy Principles Poster.* http://eli.education.govt.nz/eli-privacy/privacy-principles-poster/

What to do when parents/guardians are separated

Ministry of Education. *Professional Practice Regarding Separated Parents/Guardians.* http://www.education.govt.nz/assets/Documents/Early-Childhood/Licensing-criteria/Centre-based-ECE-services/GMA4ProfessionalPracticeRegardingSeparatedParents.pdf

Privacy Act guide for teachers

Dalziel, K. (2009). Privacy in schools: A guide to the Privacy Act for principals, teachers and boards of trustees. *Office of the Privacy Commissioner.* Wellington. http://www.privacy.org.nz/assets/.