Meeting Notes from Tautoko Network Meeting

January 2021

The Privacy Act and Volunteers

Thank you to those who attended last week's Tautoko Network meeting at which Susan from Community Law facilitated a session on the recent changes to the Privacy legislation. We are grateful for the continuing support of Community Law Canterbury who once again facilitated our first session of the year, this year sharing some 'highlights' from the updated Privacy Act.

Susan started by noting that while, yes, there are changes, there is nothing to worry about if we are aware and incorporate the relevant parts of the Privacy Act into our everyday practice.

One of the main changes is around notification of privacy breaches. Whereas in the past if you were aware of a breach, you could just talk to the volunteer affected, the requirement now can be broken down into four steps:

C - Contain: contain the breach of privacy to ensure no further breaches occur
A - Assess: assess the scope of the breach – e.g.. the extent of the information provided, how sensitive the information is, the cause of the breach, the potential harm that might result – whether the person involved is likely to be harmed, humiliated, or have their reputation relationship damaged as a result, etc)
N - Notify: If more than minimal harm could be caused, notify the volunteer. If there is a risk of serious harm, notify both the volunteer and the Office of the Privacy Commissioner.
P - Prevent: take steps to minimise the risk of a similar breach happening again in future

It is the third step - which now includes the need to notify the Privacy Commissioner's Office if there is a risk of serious harm - which is 'new' and needs to be noted going forward. How do we notify the Privacy Commissioner? https://privacy.org.nz/responsibilities/privacy-breaches/notify-us/ This link will take you through the steps of reporting a breach. Please be aware that, if a breach has or may create a risk of serious harm, reporting the breach is a requirement. The involvement of the Privacy Commissioner will act as an essential step to ensure that action has been taken which is appropriate in the circumstances and which will mitigate the risk of a similar breach happening in the future. It also shows the Privacy Commissioner that you have thought through the processes and identified how to improve.

An example of a breach which we may come across in our volunteer management roles could be the hacking of data held which includes the holding of copies of drivers' licences. The inadvertent disclosure of information from personal identification documents such as drivers' licences and passports is a serious breach as details contained on those documents are used in cases of 'identity theft'.

As a first step, then, consider whether you are currently collecting only information you need for the actual role. Perhaps you have to 'sight' a driver's licence – so, sign off your paperwork that you have sighted it, and hand the driver's licence back. If a copy needs to be retained for a short time, keep it for only as long as is required and then promptly shred or delete the copy. If there is a need (perhaps for funding purposes) to keep copies of such personal identification material on an ongoing basis, then be clear that this requirement is recorded as the reason for retaining the information. Personal information on volunteers should be treated in the same way as that of paid staff. Take care to ensure that any available safeguards (such as passwording and/or encryption and/or partitioning of a drive with limited rights of access) is used for any HR related documentation. If you have any doubts about whether documentation should be retained, check with the Privacy Commissioner's office.

Susan provided an excellent and very relevant scenario which formed the basis of some great discussion around the table – providing references for volunteers. Increasingly, as many of you are experiencing, volunteers are utilising their engagement in the community as a stepping stone to paid employment and will often ask an organisation, or their volunteer manager, for a reference. With the Privacy Act in mind, what do you need to know?

- Get the permission from the volunteer to give the information/reference
- Verify the identity of the person requesting the information/reference. Asking them to send the questions through via email may also help to enable you to satisfy yourself that the enquirer is genuine.
- Agree, at the beginning of the conversation or email exchange that the reference is 'to be provided in confidence'.
- Check if you/your organisation has the information requested – you can only comment on what you know (it may be, for example, that you are not the best person within the organisation to be providing the reference)
- Keep a record of what was discussed. If it was agreed that the reference was to be provided "in confidence", then you will not be required to provide details of that conversation if requested to do so under the Privacy Act.

Employers or HR recruiters may ask questions that breach privacy laws – such as those relating to the mental health of the applicant. Not comfortable with the question? Suggested answer: "certainly for the role that XYZ performs for our organisation, there is no concern re medical/mental health issues"

Tip: if you are sending through a document, perhaps in the case of a complaint, and wish not to identify the person/s involved, do not rely on just a black marker to cover the relevant names. Once photocopied, scanned, and maybe copied again, the name may still be visible. Use correcting tape or a piece of paper to completely the cover the material you do not wish to be shared. Useful tips on how to effectively redact information from a document is available

here: https://www.wikihow.com/Redact-a-Document

Privacy Officer – does your organisation have a Privacy Officer? Yes, you do need one. The Privacy Officer is responsible for things such as dealing with privacy information requests, dealing with privacy breaches, vetting of volunteers, and acts as the link with the Privacy Commission and any person with a privacy related issue. If your organisation doesn't have a Privacy Officer, your Board should pass a resolution that the role is established and move to fill it (and budget for any training that person may require). Volunteering Canterbury is working on a role description which will be added to our 'resources' on the website, www.volcan.org.nz.

How long should information be kept? – volunteers personal information should not be kept any longer than is necessary. However, there are rules around the length of time which certain volunteer records need to be kept (e.g., expense reimbursement records need to be kept for 7 years from the end of the relevant financial year; health and safety incident records need to be kept for 5 years from the end of the year in which any health and safety incident occurred).

Remember: if records should only be kept a certain length of time, they must be deleted in any format in which they are held – not just paper copies!