MINISTER FOR CHILD PROTECTION — PORTFOLIOS — MOBILE DEVICES

3177. Mr Z.R.F. Kirkup to the Minister for Child Protection; Women's Interests; Prevention of Family and Domestic Violence; Community Services:

In respect of the Minister's portfolio responsibilities for any of their departments, agencies, government trading enterprises or boards, I ask:

(a) Are there any policies or procedures in place for restricting unauthorised access to mobile devices (mobile phones, tablets and laptops):

  (i) If so, what are they; and

  (ii) If not, why not;

(b) How many mobile devices have been disposed of in the following financial years and what was their disposal method (i.e. at auction):

  (i) 2015–16;

  (ii) 2016–17; and

  (iii) 2017–18; and

(c) Were any of the mobile devices in (b)(i)–(iii) used to store sensitive or confidential information:

  (i) If so, what type of sensitive or confidential information; and

  (ii) If so, what measures are put in place to ensure this information is not retained on the hard-drive of the device upon it's disposal?

Ms S.F. McGurk replied:

This answer covers multiple Ministers' portfolios, including Disability Services, Volunteering, Seniors and Ageing, Housing, Youth, Veterans Issues, as well as my Child Protection, Women's Interests, Prevention of Family and Domestic Violence and Community Services portfolios

(a) Yes;

  (i) The Department of Communities Administration Manual outlines the procedure for restricting unauthorised access to mobile devices. Users issued with Department of Communities mobile devices are required to take reasonable precautions to keep them physically secure and protected from unauthorised access. In the event of loss or theft, access to mobile devices is automatically restricted.

  (ii) Not applicable.

(b) Devices for disposal are sent to a third party facility for recycling under common use agreement WAS2016.

  (i) 2015–16: 215

  (ii) 2016–17: 718

  (iii) 2017–18: 451

(c) Yes.

  (i) In the normal course of business, the Department of Communities may have a variety of corporate and client information securely stored on mobile devices as part of business applications emails or within applications.

  (ii) Data on hard drives are sanitised in accordance with US Department of Defence 5220.22-M standards or destroyed and a certificate of destruction is issued. Devices are reset to factory default and recycled under common use agreement WAS2016 and a certificate of destruction issued to the Department of Communities. Any devices that are unable to be wiped are physically destroyed.