MINISTER FOR EDUCATION AND TRAINING — PORTFOLIOS — MOBILE DEVICES

3190. Mr Z.R.F. Kirkup to the minister representing the Minister for Education and Training:

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?

Mr P. Papalia replied:

Department of Education

(a) Yes.

  (i) ICT Security Policy and Telecommunications Use Policy

  (ii) Not applicable.

(b) (i)–(iii) It is not possible to provide a response without a comprehensive school survey as mobile device acquisition and disposal is a local school decision. The disposal of devices is managed through the Department of Finance's Common Use Arrangement CUAWAS2016 for Waste Disposal and Recycling, Category E.

(c) (i)–(ii) It is not possible to provide a response without a comprehensive school survey. The Department provides schools and business units with detailed advice on the disposal of various devices, including mobile devices on the Intranet. This includes advice and guidance for ensuring that data cleansing processes are completed.

Department of Training and Workforce Development

(a) Yes.

  (i) Mobile Service and Device Use Policy V3.0

  Mobile Device Management Solution (enforcing passcode settings, device tracking and remote wiping)

  Digital Information Security Policy V4.0

  (ii) Not applicable.

(b) Common Use Arrangement WAS2016 Waste Disposal and Recycling Services – ICT Disposal procedure using "Blanco" software – HMG Infosec Standard 5, Higher Standard

  (i) Nil.

  (ii) 72

  (iii) Nil.

(c) Yes.

  (i) Work emails, corporate documents

  (ii) Common Use Arrangement WAS2016 Waste Disposal and Recycling Services – ICT Disposal procedure using "Blanco" software – HMG Infosec Standard 5, Higher Standard

North Regional TAFE

(a) Yes.

(i) Information Systems Usage Policy

(ii) Not applicable.

(b) Prior to 11 April 2016, there were 11 TAFE colleges (known as State Training Providers) which had no central repository. As a result, the current TAFE colleges can only report from 11 April 2016 onwards.

Common Use Arrangement WAS2016 Waste Disposal and Recycling Services – ICT Disposal procedure using "Blanco" software – HMG Infosec Standard 5, Higher Standard

(i) 12

(ii) 9

(iii) 6

(c) Yes.

(i) Email and calendar information

(ii) Devices are cleared and returned to default factory settings prior to disposal, and the destruction of storage (HDD, SSD, NAND) device.

Central Regional TAFE

(a) Yes.

(i) Policy and Procedure for Mobile Data and Communication Services (AF010P)

Mobile Data and Communication Devices Employee Ageement (AF010F1)

(ii) Not applicable.

(b) Prior to 11 April 2016, there were 11 TAFE colleges (known as State Training Providers) which had no central repository. As a result, the current TAFE colleges can only report from 11 April 2016 onwards.

Common Use Arrangement WAS2016 Waste Disposal and Recycling Services – ICT Disposal procedure using "Blanco" software – HMG Infosec Standard 5, Higher Standard

(i) Nil.

(ii) Nil.

(iii) Nil.

(c) Yes.

(i) Work emails.

(ii) Devices are cleared / wiped and returned to factory settings prior to disposal.

South Metropolitan TAFE

(a) Yes.

(i) Information and Communications Technology (ICT) Information Security Policy

ICT Mobile Device Policy (Including requirement for password protection)

Mobile Device Access Procedure

Mobile Device Users Agreement Form

ICT Access Control Policy

(ii) Not applicable.

(b) Prior to 11 April 2016, there were 11 TAFE colleges (known as State Training Providers) which had no central repository. As a result, the current TAFE colleges can only report from 11 April 2016 onwards.

Common Use Arrangement WAS2016 Waste Disposal and Recycling Services – ICT Disposal procedure using "Blanco" software – HMG Infosec Standard 5, Higher Standard

(i) 25

(ii) 136

(iii) 218

(c) Yes.

(i) Mobile devices were used to access email content which may or may not store sensitive or confidential information

(ii) Devices are cleared and returned to default factory settings prior to disposal

South Regional TAFE

(a) Yes.

(i) Mobile Phone and Devices Procedure and Request

(ii) Not applicable.

(b) Prior to 11 April 2016, there were 11 TAFE colleges (known as State Training Providers) which had no central repository. As a result, the current TAFE colleges can only report from 11 April 2016 onwards.

Common Use Arrangement WAS2016 Waste Disposal and Recycling Services – ICT Disposal procedure using "Blanco" software – HMG Infosec Standard 5, Higher Standard

(b) (i) 2

(ii) 5

(iii) 11

(c) Yes.

(i) Mobile devices were used to access email content which may or may not store sensitive or confidential information.

(ii) Devices are cleared and returned to default factory settings prior to disposal.

North Metropolitan TAFE

(a) Yes.

(i) Telecommunications Management, Control and Usage Policy

(ii) Not Applicable

(b) Prior to 11 April 2016, there were 11 TAFE colleges (known as State Training Providers) which had no central repository. As a result, the current TAFE colleges can only report from 11 April 2016 onwards.

Common Use Arrangement WAS2016 Waste Disposal and Recycling Services – ICT Disposal procedure using "Blanco" software – HMG Infosec Standard 5, Higher Standard

(i) 0

(ii) 65

(iii) 173

(c) Yes.

(i) Devices used to access email content, financial information, staff and student information and contract information.

(ii) Hard disks and electronic media are sanitized before disposal as indicated on the ITS Sanitising of Hard Disks and Electronic Media Storage Procedure P052R, the sanitizing is documented on the Asset Disposal Form W1082C1

Building and Construction Industry Training Fund

(a) Yes.

(i) Information Technology – Terms of Use and Security Policy

Social Media Policy and Guidelines

Human Resources Management Manual

(ii) Not applicable.

(b) Recycling and staff silent auction.

(i) 0

(ii) 3

(iii) 1

(c) No.

(i) Not applicable.

(ii) Not applicable.