Direction under s. 41(1) of the Privacy and Personal Information Protection Act 1998 in relation to the Department of Education

As Privacy Commissioner appointed under Part 4, Division 1 of the *Privacy and Personal Information Protection Act 1998* ("the PPIP Act"), I, Samantha Gavel, hereby direct, pursuant to section 41(1) of the PPIP Act that:

1 Overview

This is a direction made under section 41(1) of the *PPIP Act*. It should be read in conjunction with the PPIP Act.

2 Interpretation

2.1 In this Direction, the following words have their respective meanings:

"Affected Individuals" means the individuals whom the Department is proposing to notify of the occurrence of a cyber security incident.

"ADC" means the Australian Death Check service.

"**QBDM"** means the Queensland Registry of Births, Deaths and Marriages.

"Department" means the Department of Education.

"IPP" means the Information Protection Principle set out in the section of the *PPIP Act* with the corresponding number.

"Personal information" has the same meaning as in s. 4 of the *PPIP Act*.

"PPIP Act" means the *Privacy and Personal Information Protection Act 1998*.

3 Background

(a) The Department is a public sector executive agency, and listed in Schedule 1 of the *Government Sector Employment Act 2013*.

(b) The ADC service is a joint initiative of all state and territory government Births Deaths and Marriages registries that offers a single source of truth of national death data for Australia.

(c) QBDM is the appointed Australian Coordinating Registry for the ADC, and has the approval of all Australian Registry of Births, Deaths and Marriages offices to provide services accessing the ADC data to an approved applicant.

(d) QBDM is part of the Queensland Department of Justice and Attorney-General which, pursuant to the *Administrative Arrangements Order (No. 2) 2021* (Qld), is an administrative unit of the Queensland government.

4 Objectives of this Direction

4.1 The Department was recently the victim of a cyber attack that has potentially compromised the personal information of the Affected Individuals.

4.2 The Department wants to contact Affected Individuals for the purpose of notifying them of the potential compromise of their personal information and providing them with assistance to respond to the potential compromise of their personal information.

4.3 The Department is concerned that if it provides notice to Affected Individuals who are deceased, that notice will be received by the deceased Affected Persons' family members, which creates a risk of causing psychological harm and distress to those family members.

4.4 In order to avoid that risk, the Department wishes to obtain access to the death status of Affected Individuals using information held by the ADC.

5 Process

5.1 QBDM will provide the Department with access to a web-based portal it has created to enable users to obtain information from the ADC records.

5.2 The Department will upload a comma separated value (.csv) file to the portal which contains the following information:

(a) a unique reference number the Department has allocated to each Affected Individual; and

(b) the given name, surname and date of birth of each Affected Individual.

5.3 The uploaded csv file is encrypted in real-time by ADC via a HMAC SHA-256 encryption algorithm using a base 64 encoded hash key. This encryption prevents the original values in the data being identified.

5.4 The hashed data is temporarily stored to disk by ADC before data matching starts (that is, matching the hashed values to the death record data held by ADC). Once the data matching starts, the hashed data is permanently deleted by ADC.

5.5 The original unencrypted data is not:

(a) accessible to QBDM or ADC at any point in time;

(b) stored on QBDM's systems, including not being stored in a log or back up.

5.6 When the portal has completed the matching, it will create a link to a file which can be downloaded from the portal by the Department. The downloaded file:

(a) only includes records where a match is obtained. Records where a match is not found are not included in the results file;

(b) only contains the unique reference number, and no other information included in the original csv file uploaded to the portal by the Department; and

(c) is only available for downloading for a short period of time of approximately four hours, after which time it is deleted.

5.7 The Department will remove, from the list of Affected Individuals to whom it will be notifying, the Affected Individuals identified by the ADC data matching as having died.

6 Public Interest

6.1 This Direction has been made to permit the collection and use of personal information by the Department for the purposes of the Department obtaining the death status for the Affected Individuals, whose personal information was affected by the cyber-attack on the Department.

6.2 Obtaining the death status of Affected Individuals will allow the Department to avoid notifying deceased Affected Individuals, and therefore avoid causing psychological harm or distress to

the family members of deceased Affected Individuals that would otherwise occur following their receipt of a notification to the deceased Affected Individual.

6.3 The public interest in permitting the collection and use of personal information, in circumstances that might not otherwise be authorised by the *PPIP Act*, is the avoidance of that psychological harm or distress.

6.4 That public interest is served by enabling the collection of the latest information about the death status of the Affected Individuals by the Department from QBDM.

6.5 The public interest in the Department complying with the relevant IPPs is outweighed by the public interest in permitting it to collect information to enable the Department to avoid psychological harm or distress to family members of deceased Affected Individuals.

7 Information exchange agreements

7.1 The Department will enter into an agreement with QBDM documenting the roles and responsibilities of each party, including data security arrangements and data retention.

8 Breach

8.1 If the Department collects, uses or discloses personal information other than in accordance with this Direction or the IPPs, the Department must notify the NSW Privacy Commissioner within 48 hours of confirmation that such a contravention has occurred.

9 Reporting and Auditing

9.1 The Department will report to the NSW Privacy Commissioner on compliance with this Direction, including the following matters:

(a) details of any complaints received from the public regarding the collection and use of personal information under this Direction; and

(b) in accordance with paragraph 8.1, any data breaches arising from this Direction involving personal information, or where breaches could have arisen.

10 Duration

10.1 This Direction has effect from the date of this direction until **28 February 2022.**

11 Non-Compliance with Information Protection Principles

11.1 The Department is not required to comply with the information protection principles under Division 1, Part 2 of the *PPIP Act* to the extent described below.

11.2 **IPP 2:** Notwithstanding s. 9 of the *PPIP Act*, the Department is not required to collect personal information about the death status of Affected Individuals directly from the Affected Individuals, but s. 9 otherwise applies to it.

11.3 **IPP 9:** Notwithstanding s. 16 of the *PPIP Act*, the Department is not required to take steps to ensure that personal information used by it for the purposes of obtaining death records of the Affected Individuals, or for the purpose of contacting the Affected Individuals, is accurate, up to date, complete and not misleading, but s. 16 otherwise applies to it.

11.4 **IPP 10:** Notwithstanding s. 17 of the *PPIP Act*, the Department is permitted to use personal information about the Affected Individuals for the purposes of obtaining death records of the Affected Individuals, and for the purpose of contacting the Affected Individuals, but s. 17 otherwise applies to it.

Signed by me on 27 January 2022

[redacted]

Samantha Gavel
Privacy Commissioner