Privacy Impact Assessment Template

Part 1 – General Description

Name of Program:	Teach Your Monster to Read		
Date:	March 19, 2018		
Name of Organisation:	Melton West Primary School		
PIA Drafter:	Jayden Spudvilas-Powell		
Email:	spudvilas-powell.jayden.l@edumail.vic.gov.au	Phone:	(03) 9743 5818
Program Manager:	Jayden Spudvilas-Powell		
Email:	spudvilas-powell.jayden.l@edumail.vic.gov.au	Phone:	(03) 9743 5818
Are you a law enforcement agency as defined in Section 3 of the PDPA? Y/N			

Definition – Program

For the purpose of this document, program will be used to mean any system, legislation, project, initiative or activity.

1. Description of the Program and Parties

Teach your Monster to Read is a series of free games designed for young children to practise the first stages of reading. Combining top quality games design with essential learning, "First Steps" and "Fun With Words" are built on the principles of synthetic phonics and follow the teaching sequence of the Letters and Sounds.

2. Scope of this PIA and any Related Privacy Impact Assessments

The Privacy Impact Assessment for Teach Your Monster to Read will cover the login details of students and identifiable information contained within the protected teacher and administration portals within the online interface.

3. Identifying Information Elements

Teach Your Monster to Read uses the following identifying information elements: unique identifiers (usernames); students' first names; students' surnames; name of the school; students' year levels; and students' class names.

3.1 Personal Information

When assessing impacts to privacy the first consideration is whether any personal information will be involved in the program. Section 3 of the PDPA defines personal information as follows:

Definition – Personal Information

Personal information means information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information of a kind to which the Health Records Act 2001 applies.

3.2 Sensitive Information

The PDPA contains specific provisions relating to the collection of sensitive information (IPP 10). While there are many types of information that attract a heightened duty of care, for example banking details, the IPPs that specifically apply to sensitive personal information in the PDPA only apply to those in the table below.

Table 1: Sensitive Information

a	Racial or ethnic origin	No
b	Political opinions	No
c	Membership of a political association	No
d	Religious beliefs or affiliations	No
e	Philosophical beliefs	No
f	Membership of a professional or trade association	No
g	Membership of a trade union	No
h	Sexual preferences or practices	No
i	Criminal record	No
This program will not collect, use or disclose any of the above information		

3.3 Unique Identifiers

The PDPA has specific requirements for the collection, use and disclosure of unique identifiers (IPP 7). The PDPA defines a unique identifier as follows:

Definition – Unique Identifier

Unique identifier means an identifier (usually a number) assigned by an organisation to an individual to uniquely identify that individual for the purposes of the operations of the organisation but does not include an identifier that consists only of the individual's name, but does not include an identifier within the meaning of the Health Records Act 2001.

An example of a unique identifier is a tax file number, a driver's license number, a passport number or a Centrelink Customer Reference Number. For further guidance on what constitutes a unique identifier please see CPDP's information sheet *'Unique Identifier' under the Privacy and Data Protection Act 2014*.

Table 2: Unique Identifiers

1	Will this program assign a unique identifier? Y/N
If YES, please explain how the unique identifier is necessary for the program: • Students will be given a unique identifier used to log into Teach Your Monster to Read • The username given to students will be the same as their first name, e.g. 'John' • Students will have a randomly generated password that matches their account • The unique identifier is necessary to enable students to access personalised reading tasks and their data history, as well as protect their data from internal or external privacy breaches.	
2	Will this program collect, use or disclose a unique identifier created by another organisation? Y/N
If YES, please describe the unique identifier, specify the organisation from which the identifier came, and the reason the identifier is necessary for your organisation to carry out its functions: **N/A**	

3.4 Health Information

While the PDPA does not apply to health information, the privacy protections that should be considered are comparable to those necessary for personal information under the PDPA. This is demonstrated by the similarity between the IPPs and the HPPs contained in the HRA.

Definition – Health Information

The HRA defines health information as:

a) information or an opinion about-

(i) the physical, mental or psychological health (at any time) of an individual; or

(ii) a disability (at any time) of an individual; or

(iii) an individual's expressed wishes about the future provision of health services to him or her; or

(iv) a health service provided, or to be provided to an individual – that is also personal information; or

b) other personal information collected to provide, or in providing, a health service; or

c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or

d) other personal information that is genetic information about an individual in a form which is or could be predictive of the health (at any time) of the individual or of any of his or her descendants – but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of this Act generally or for the purposes of specified provisions of this Act.

Table 3: Health Information

1	Will this program collect, use or disclose health information? Y/N
If YES, please describe the health information: **N/A**	

3.5 Re-identifiable Information

Definition – De-identified

The PDPA defines the term de-identified, in relation to personal information as meaning that the information no longer relates to an identifiable individual or an individual who can be reasonably identified.

Many programs rely on the use of de-identified or non-identifiable information. When such information is used it needs to be treated with caution and afforded many of the same privacy protections as personal information, where there is the potential for re-identification to occur. This is particularly the case where a program involves data matching/linking activities. For that reason, when assessing privacy of personal information, potentially re-identifiable information should be protected in the same way as personal information.

The National Health and Medical Research Council of Australia provides the following definitions, which should assist in determining when information should be considered re-identifiable (https://www.nhmrc.gov.au/book/glossary).

Definition – Re-identifiable Data

Re-identifiable data is data from which identifiers have been removed and replaced by a code, but it remains possible to re-identify a specific individual by, for example, using the code or linking different data sets.

Definition – Non-identifiable Data

Non-identifiable data is data that has never been labelled with individual identifiers or from which identifiers have been permanently removed, and by means of which no specific individual can be identified. Subsets of non-identifiable data are those that can be linked with other data so it can be known they are about the same data subject, although the person's identity remains unknown.

Table 4: Re-identifiable Information

1	Will this program collect, use or disclose re-identifiable information? Y/N
If YES, please describe the process of de-identification and potential for re-identification: **N/A**	

Table 5: Threshold Assessment

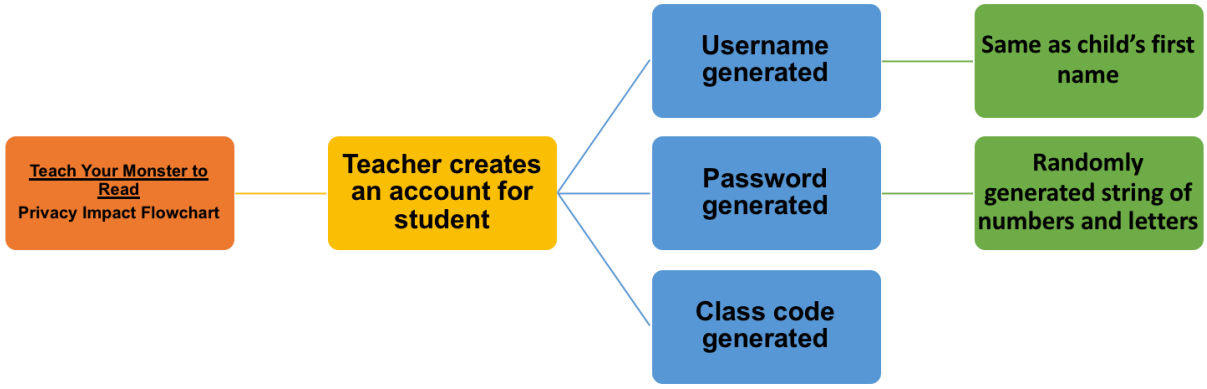
Based on the information above, does your program collect, use or disclose:		Y	N
1	Personal information (which may include any of sensitive information, unique identifiers, re-identifiable information or health information)? *If YES, please proceed with the rest of the assessment.* *If NO, continue to sign off page.*	✓	
2	Health information ONLY (and no other types of personal information)? *If YES, please proceed to sign off page and consider your obligations under the HRA. Please contact the Health Services Commissioner for further assistance.* *If NO, please proceed with the rest of the assessment.*		✓
3	Personal information (including sensitive information, unique identifiers, re-identifiable information) AND health information? *If YES, please proceed with the rest of this assessment and consider your obligations under the HRA. Please contact the Health Services Commissioner for further assistance.*		✓

Table 6: Legal Authority

1	If you have legal authority under your organisation's enabling legislation to collect, use or disclose personal information for the purposes of this program, please cite the relevant legislation and section within that act and continue with the assessment. If your enabling legislation does not explicitly permit or require the collection, use or disclosure of the information, please proceed with the rest of the assessment.
Relevant legislation: • Melton West Primary School – ICT Acceptable Use Policy (http://meltonwestps.vic.edu.au/our-school/#policies) • Melton West Primary School – Digital Backpack P-2 (http://meltonwestps.vic.edu.au/wp-content/uploads/sites/133/2016/07/MWPS-Digital-Backpack-P-2.docx) • Melton West Primary School – Digital Backpack 3-6 (http://meltonwestps.vic.edu.au/wp-content/uploads/sites/133/2016/07/MWPS-Digital-Backpack-3-6.docx)	

2.1 Information Flow Table/Diagram

Teach Your Monster to Read: Privacy Impact Flowchart at Melton West Primary School



2.2 Information Privacy Principles

Collection of Personal Information (including sensitive information and unique identifiers) *(Refer to IPPs 1, 7, 8 & 10)*

Collection		Y	N	IPP
1	Is all the information collected NECESSARY for the program?	✓		1.1
2	Is it lawful or practicable for the individual to remain anonymous for the purpose of the program?		✓	8.1

Risk Identifier: If the answer to question 1 is NO, please address Collection as a risk in Part 3 – Privacy Risk Mitigation. If the answer to question 2 is YES and the program will collect personal information, please address Anonymity as a risk in Part 3 – Privacy Risk Mitigation.

Notice				
3(a)	Have you taken reasonable steps to ensure that the individual whose information is collected is made aware of the information below? Have you taken reasonable steps to ensure that the individual whose information is collected is made aware of the information below? • The identity of the organisation and how to contact it • The fact that the individual can access their information • The purpose for the collection • To whom the organisation will disclose the information • Any law requiring the information to be collected • Consequences, if any, to the individual if the information is not provided. *If YES, please describe how:* • Disseminating the *ICT Acceptable Use Agreement* and *Digital Backpack* pertinent to the child's year level at the start of the year • Publishing the Privacy Impact Assessment on Teach Your Monster to Read on the Melton West Primary School website that details the privacy implications of the program • Teachers and students engaging in classroom discussions about how Teach Your Monster to Read will be used for teaching and learning purposes at the school and how/why teacher and student information is collected (if the service is being used in the classroom).	✓		1.3
3(b)	If the answer to question 3(a) is NO, is the collection done by a law enforcement agency for a law enforcement function or activity? (For further information see Section 15 of the PDPA).			

Risk Identifier: If the answers to questions 3(a) and (b) are both NO please address Notice as a risk in Part 3 – Privacy Risk Mitigation.

Direct/Indirect Collection				
4(a)	Is the information being collected DIRECTLY from the individual? *If NO, proceed to question 4(c).*	✓		1.4
4(b)	Will any information also be collected INDRECTLY about the individual? *If NO, proceed to question 5.*		✓	
4(c)	*If the answer to question 4(a) is NO or the answer to question 4(b) is YES, please check the exception to the notice requirement that applies.*			
	Reasonable steps have been taken to ensure the individual whom the information is about has been made aware of the information in question 3; OR			1.5
	It would pose a serious threat to the life or health of any individual if the matters in question 3 were communicated to the individual			
	The collection is by a law enforcement agency for a law enforcement function or activity (for further information see Section 15 of the PDPA).			

Risk Identifier: If the answers to questions 4(a) and (b) are all NO, please address Indirect Collection as a risk in Part 3 –

Privacy Risk Mitigation.

Unique Identifier				
5(a)	Will this program assign or collect a unique identifier (see Table 2 above). *If NO, proceed to question 6.*	✓		
5(b)	Is it NECESSARY to assign a unique identifier to enable your organisation to carry out its program?	✓		7.1
5(c)	Will a unique identifier of another organisation be used ONLY if one of the following conditions is met?	✓		7.2
	It is necessary for your organisation to carry out its functions (this should be described in Table 2 above); OR			
	The individual has consented to the use; OR			
	It is an outsourcing organisation adopting the unique identifier of a CSP performing obligations under a state contract			
5(d)	An individual will not be required to provide a unique identifier unless authorised by law or in connection with the purpose for which the unique identifier was originally assigned. *If YES, please explain:* • Melton West Primary School will disseminate the unique identifier and associated password to students so that they can log into Teach Your Monster to Read at school and access their learning data.	✓		7.4
Risk Identifier: If the answers to questions 5(b)-(d) are all NO, please address Unique Identifiers as a risk in Part 3 – Privacy Risk Mitigation.				
Sensitive Information				
6(a)	Will this program collect sensitive information (see Table 1 above). *If NO, proceed to question 7.*		✓	
6(b)	Sensitive information identified in Table 1 will not be collected unless one of the following apply:			10.1
	The individual has consented			10.1(a)
	The collection is required under law			10.1(b)
	The collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual that the information is about is physically or legally incapable of consenting or physically cannot communicate the consent			10.1(c)
	The collection is necessary for the defence of a legal or equitable claim			10.1(d)
	The collection is necessary for research, compilation or analysis of statistics for a government funded welfare or educational service OR if relating to racial or ethnic origin, the information is collected for providing government funded welfare or educational services; AND There is no reasonably practicable alternative to collecting the sensitive information for that purpose; AND It is impracticable for the individual to consent.			10.2(a)(i) 10.2(a)(ii) 10.2(b) 10.2(c)

Risk Identification: If the answer to question 6(b) is NO, please address Sensitive Information as a risk in Part 3 – Privacy Risk Mitigation.

Use and Disclosure of Personal Information *(Refer to IPPs 2 & 7)*

Use and Disclosure		Y	N	IPP
7	Information will ONLY be used or disclosed for the primary purpose identified in Part 1. *If YES, proceed to question 9.*	✓		2.1
8(a)	In addition to using and disclosing information for the primary purpose it was collected, personal information will be used or disclosed for a secondary purpose. *If YES, please check which of the following secondary purposes below apply (8(b)-8(j)):*			
8(b)	a) The secondary purpose is related to the primary purpose, or for sensitive information, directly related to the primary purpose; AND b) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose *If YES, please describe the secondary purpose:*			2.1(a)
8(c)	The individual has consented (express or implied) to the use or disclosure			2.1(b)
8(d)	As necessary for research, or the compilation or analysis of statistics IN THE PUBLIC INTEREST			2.1(c)
8(e)	Where necessary to lessen or prevent a serious and imminent threat to an individual's life, health, safety or welfare; or a serious threat to public health, public safety or public welfare			2.1(d)
8f)	Where necessary on suspicion or unlawful activity as part of its investigation or reporting its concerns to relevant persons or authorities			2.1(e)
8(g)	As required or authorised by law *If YES, please site the relevant law:*			2.1(f)
8h)	By or on behalf of a law enforcement agency for one of the following purposes: (* a written note must be made of any use or disclosure made under this section)			2.1(g)/ 2.2
	(i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction			
	(ii) the enforcement of laws relating to the confiscation of the proceeds of crime			
	(iii) the protection of the public revenue			
	(iv) the prevention, detection, investigation or remedying of seriously improper conduct			
	(v) the preparation or conduct of proceedings or implementation of the orders of any court or tribunal			
8(i)	As requested, in writing by the Australian Security Intelligence Organisation (ASIO) or the Australian Secret Intelligence Service (ASIS)			2.1(h)
8(j)	The use or disclosure is by a law enforcement agency for a law enforcement			

	function or activity (for further information see Section 15 of the PDPA)			

Risk identification: If the answer to question 8(a) is YES and 8(b)-(j) are all NO please address Secondary Purpose as a risk in Part 3 – Privacy Risk Mitigation.

Use and Disclosure of a Unique Identifier (assigned by another organisation)		Y	N	IPP
9(a)	This program will use or disclose a unique identifier assigned to an individual by another organisation (see Table 2 above). *If NO, proceed to question 10.*		✓	7.2
9(b)	The unique identifier assigned to an individual by another organisation will not be used or disclosed unless one of the following apply:			7.3
9(c)	It is necessary for the organisation to fulfil its obligation to the other organisation			7.3(a)
9(d)	The individual has consented			7.3(c)
9(e)	One or more of the following apply: (see IPP 2.1(d)-(g) for full conditions)			7.3(b)
9(f)	A serious threat to individual or public health, safety or welfare			
9(g)	Reporting a suspected unlawful activity to the relevant person or authority as part of an investigation			
9(h)	It is required or authorised by law *If YES, please site the relevant law:*			
9(i)	The organisation reasonably believes the use or disclosure is reasonably necessary by or on behalf of a law enforcement agency (see IPP 2.1(g) for full description)			

Risk Identifier: If the answer to question 9(a) is YES and 9(c)-(i) are all NO please address Unique Identifiers as a risk in Part 3 – Privacy Risk Mitigation.

***Transborder Data Flows** (Refer to IPP 9)*

Transborder Data Flows		Y	N	IPP
10(a)	The program will transfer personal information to an organisation or person outside of Victoria (other than the organisation or the individual). *If NO, proceed to question 11. If YES, please describe:*		✓	
10(b)	Personal information will only be transferred to someone outside of Victoria (other than the organisation or the individual) if one of the following (10(c)-10(h)) apply:			9.1
10(c)	The organisation reasonably believes that the recipient is subject to laws or a contract enforcing information handling principles substantially similar to the IPPs			9.1(a)
10(d)	The individual consents to the transfer			9.1(b)
10(e)	The transfer is necessary for the performance of a contract between the individual and the organisation			9.1(c)
10(f)	The transfer is necessary as part of a contract in the interest of the individual between the organisation and a third party			9.1(d)
10(g)	All of the following apply: The transfer is for the benefit of the individual; AND It is impractical to obtain consent; AND If it were practicable the individual would likely consent.			9.1(e)

10(h)	The organisation has taken reasonable steps so that the information transferred will be held, used and disclosed consistently with the IPPs *If YES, please describe steps:*			9.1(f)

Risk Identification: If the answer to question 10(a) is YES and 10(c)-(h) are all NO please address Transborder Data Flows as a risk in Part 3 – Privacy Risk Mitigation.

***Data Quality** (Refer to IPP 3)*

Data Quality	IPP 3.1
Steps taken to ensure that all data that is collected, used or disclosed will be accurate, complete and up to date: • Student information (e.g. first names, surnames) obtained from CASES21 • Accuracy of student information reviewed by the classroom teacher on a needs basis • Exited and graduated students are removed from Teach Your Monster to Read by the classroom teacher on a needs basis • Classroom teachers are coached in the use of Teach Your Monster to Read and the analysis and protection of learning data by the Digital Pedagogies Leading Teacher • Teachers are required to report incidents and privacy breaches on Teach Your Monster to Read to the Digital Pedagogies Leading Teacher, relevant Assistant Principal and the Principal of Melton West Primary School immediately.	

Risk Identification: If the program does not ensure that all data collected, used or disclosed is accurate, complete and up to date, please address Data Quality as a risk in Part 3 – Privacy Risk Mitigation.

***Security of Personal Information** (Refer to IPP 4)*

IPP 4 requires an organisation to take reasonable steps to protect the personal information it holds from misuse, loss and unauthorised access, modification and disclosure. The Victorian Protective Data Security Framework (VPDSF) provides guidance on data security for the Victorian public sector. Compliance with the VPDSF is considered to constitute 'reasonable steps' under IPP 4.1.

Data Security		**Y**	**N**	**IPP**
12(a)	The program has taken reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure. Reasonable steps includes undertaking the following activities across the information lifecycle: • identifying and understanding information types • assessing and determining the value of the information • identifying the security risks to the information • applying security measures to protect the information • managing the information risks. For more information on these requirements please refer to the data security resources available on the CPDP website.	✓		4.1 & VPDSF

Risk Identification: If reasonable steps have not been taken to protect personal information please address Data Security as a risk in Part 3 – Privacy Risk Mitigation.

Records Management		Y	N	IPP
12(b)	The program will take reasonable steps to destroy or de-identify personal information if it is no longer needed for any purpose. *If YES, please list the steps or the relevant records Retention and Destruction Authority (RDA) under the Public Records Act 1973.* • Information of exited students deleted by the classroom teacher on a needs basis.	✓		4.2
Risk Identification: If the answer to question 12(b) is NO, please address Records Management as a risk in Part 3 – Privacy Risk Mitigation.				

***Openness** (Refer to IPP 5)*

Openness		Y	N	IPP
13(a)	The organisation has a document available for public review that sets out the policies for the management of personal information. *Please identify document(s) and provide link where available:* • Melton West Primary School – ICT Acceptable Use Policy (http://meltonwestps.vic.edu.au/our-school/#policies) • Melton West Primary School – Digital Backpack P-2 (http://meltonwestps.vic.edu.au/wp-content/uploads/sites/133/2016/07/MWPS-Digital-Backpack-P-2.docx) • Melton West Primary School – Digital Backpack 3-6 (http://meltonwestps.vic.edu.au/wp-content/uploads/sites/133/2016/07/MWPS-Digital-Backpack-3-6.docx).	✓		5.1
13(b)	The organisation has steps in place to allow an individual to know what personal information it holds about them and for what purposes it collects, uses and discloses it.	✓		5.2
Risk Identification: If the answer to question 13(a) or (b) is NO, please address Openness as a risk in Part 3 – Privacy Risk Mitigation.				

***Access and Correction** (Refer to IPP 6)*

The Access and Correction principle (IPP 6) entitles individuals to view and obtain copies of their personal information and to correct personal information held about them. IPP 6 is designed to supplement existing access and correction rights under the *Freedom of Information Act 1982* (FOI Act). Information held by a Victorian public sector organisation is subject to the FOI Act and therefore do not need to assess against IPP 6.

Where the public sector outsources part of their program services to a CSP, the CSP will be required to comply with IPP 6 but only in relation to the CSP's provision of service under a state contract. Please refer to Outsourcing and Privacy Guidelines for additional information

on CSPs and their obligations under IPP 6.

Risk Mitigation Table					
	Identified Risk	**Mitigation Strategy**	**Likelihood**	**Impact**	**Risk Rating**
1	Students share other students' unique identifiers (i.e. usernames) and passwords with other students or family members.	- ICT Acceptable Use Policy shared with families and staff in the school - ICT Acceptable Use Policy updated on a regular basis by the Digital Pedagogies Leading Teacher and reviewed by the Principal Class - Teachers discuss and refer to the ICT Acceptable Use Policy on a regular basis - eSmart Student Leaders uphold the integrity of student privacy information in classrooms.	Medium	Medium	Medium

Part 3 – Privacy Risk Mitigation

Table 7: Risk Mitigation

For the purpose of this section, a risk is something that could lead to the unauthorised collection, use, disclosure or access to personal information.

There are a number of other risks that could arise that do not relate directly to the IPPs. For example, the risk that personal information might be produced where non-identifiable data are subject to data matching/linking or data analytics. Community expectations of how public sector organisations should use personal information are also important to consider. Even where an act or practice does not contravene the IPPs, individuals may be uncomfortable with the use of their information for particular purposes. Please consider an assessment of all risks related to personal privacy. Further, the rights and responsibilities under the Charter should also be taken into account when assessing the risks associated with the program.

It is important to note that while identifying and mitigating privacy risks is a critical component of good privacy practice, risk mitigation does not provide an alternative to compliance with the IPPs. Privacy needs to be incorporated with other program goals, such as security or functionality and not balanced against them. A public sector agency must ensure that any handling of personal information is aligned with privacy legislation and only departs from the requirements in very limited circumstances. See the *Public Interest Determinations* discussion below for acceptable departures from the IPPs.

New Risk Mitigation Option: Public Interest Determinations

The PDPA requires organisations to comply with each of the IPPs. However, where there is a public interest in an organisation not complying with one or more of the IPPs (with the exception of IPP 4 – Data Security and IPP 6 -

Access and Correction), they may apply for a public interest determination (PID). If your organisation is not compliant with one or more of the IPPs for this program, as identified by the above checklist, a PID may be appropriate if there is an overriding public interest in non-compliance. For a full discussion of PIDs, see the *Guidelines to Public Interest Determinations, Temporary Public Interest Determinations, Information Usage Arrangements and Certification*.

Part 4 – Summary of Assessment and Sign Off

Summary

- Teach Your Monster to Read creates unique identifiers (i.e. usernames and passwords) for students with personal information attached to their accounts, including first names, surnames and class names, to protect their learning data
- Melton West Primary School implements, reviews and updates relevant policies and documents pertinent to the creation and sharing of personal student information in online services and disseminates these documents to the parent/guardian community at the beginning of each school year:
    - ICT Acceptable Use Policy
    - Digital Backpack P-2
    - Digital Backpack 3-6
- The Digital Pedagogies Leading Teacher ensures that teachers and students at Melton West Primary School understand the information collected by Teach Your Monster to Read and how to protect this information from misuse
- The Digital Pedagogies Leading Teacher plays an active role in the retention of student information on Teach Your Monster to Read and abides by a schedule in adding/deleting student information on Teach Your Monster to Read as necessary
- The Digital Pedagogies Leading Teacher shares privacy insights, issues and dangers on Teach Your Monster to Read with teachers and the Principal Class as appropriate.

Signatures

Program/Department Manager	Signature	Date
Head of Public Body, or delegate	Signature	Date