Privacy and consent explained

Advice for schools – parents

The following information provides questions and answers in relation to privacy and consent matters for managing student information within online systems and digital applications in the school setting. This information is designed for both staff and parent use.

What is the *Information Act 2002*?

The Northern Territory (NT) *Information Act 2002* deals with three important aspects of the way in which the NT Government manages information:

1. Provides for public access to information held by the public sector know as Freedom of Information (FOI) which allows anyone the right to apply for access to government information.
2. Individuals can apply to correct personal information that government holds about them if it is incorrect, incomplete, or out of date.
3. Provides for the responsible collection and handling of personal information by the public sector, and to promote appropriate records and archives management.

What are the Information Privacy Principles?

Information Privacy Principles, listed in schedule 2 of the *Information Act 2002*, are the rules for protecting an individual's privacy set out in the ten Information Privacy Principles (IPP). The ten Privacy Principles are about making sure NT Government organisations respect a person's privacy when their personal information is collected or handled. The requirements can be divided into four categories: Collection and use; Use and disclosure; Management of information; Openness.

The following explanations provide a general overview. For further advice, go to the *Information Act 2002* link in the resources section.

Primary and secondary purpose (IPP2 Use and disclosure) – a public sector organisation must not use or disclose personal information about an individual for a purpose (secondary) other the primary purpose unless the secondary purpose is directly related to the primary purpose. This means the intent is that a person's personal information is used and disclosed only in the way the individual would expect.

Offshore data hosting (IPP9 Transborder data flows) – a public sector organisation must not transfer personal information about an individual to a person (other than the individual) outside the NT unless authorised under a law, transfer is necessary or the individual consents to the transfer. This means reasonable steps have been undertaken to ensure the recipient does not breach the IPP in relation to that information.

Security of Data (IPP4 Data security) – a public sector organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification, or disclosure. A public sector organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose. This means the public sector organisation must take reasonable steps to protect personal information it holds and to actively consider whether it is permitted to retain personal information. Once no longer required, reasonable steps must be taken to destroy or de-identify personal information once it's no longer needed for the purpose it is being used or disclosed. This does not apply to personal information contained in an NT Government record management system managed in line with NT Government Record Disposal Schedules.

NORTHERN TERRITORY GOVERNMENT

What is personal information?

Personal Information is government information that discloses a person's identity or from which a person's identity is reasonably ascertainable.

Government information is not personal information to the extent that the person's identity is only disclosed in the context of having acted in an official capacity for a public sector organisation and the government information discloses no other personal information about the person.

What is considered sensitive information?

Sensitive information is personal information about a person's racial or ethnic origin, political opinion, membership of a political association, religious belief or affiliation, philosophical belief, membership of a professional or trade association, membership of a trade union, sexual preferences or practices and criminal records.

Is health information the same as sensitive information?

Yes, sensitive information includes health and wellbeing information. Health Information means personal information about the physical or mental health of a person, or a person's disability.

What is the meaning of consent?

Consent is when someone voluntarily agrees for their information to be collected, used or shared within or outside the school or the Department of Education. In certain situations, privacy law requires that an organisation, for example school, needs consent to collect personal information and to use or disclose it. Consent is generally needed for the collection of a person's sensitive information or to use or disclose personal information for a purpose other than the purpose it was collected for.

Why do you ask for consent?

In line with the Information Privacy Principles and the *Education Act 2015*, consent must be provided when student information is collected, used, or transferred out of the NT where data is hosted in third party cloud service providers.

How should consent be provided?

Consent must be informed – consent is only valid if the person providing consent is made aware of the consequences of giving or not giving their consent at the time, they make the decision. An organisation, for example school, or agency should:

- clearly explain how they want to handle personal information
- communicate the request for consent in plain English, without legal or industry jargon.

Consent must be current and specific – when a person gives consent at a particular time and for specific circumstances, an organisation, for example school, or agency can't assume that the consent continues indefinitely.

When asking for consent, an organisation or agency must explain the reason for their request and be as specific as possible. They shouldn't ask for consent that is broader than necessary. For example, you shouldn't be asked to consent to undefined future use or vague statements such as all legitimate uses or disclosures.

Consent must be voluntary – voluntary consent is when you're not forced or pressured to give consent. Some factors that decide if consent is voluntary are:

- the options available if a person chooses not to provide consent; and
- the seriousness of any consequences to a person, their family, or associates if they refuse to consent.

Capacity to give consent – this means that a person:

- understands they are being asked to decide to give or not give consent;
- understand the consequences of giving or not giving consent;
- can base their decision on reason; and
- can communicate their decision.

Note: where there is uncertainty about an individual having capacity to provide informed consent, the offer of support such as interpreter or discussion where practical should be made available.

Are there different types of consent?

Yes, there are different types of consent, explained as follows.

Implied consent – is when an organisation doesn't need a person's express consent to handle non-sensitive personal information, but they need to reasonably believe that they have implied consent. It's not sufficient for an organisation simply to tell you of their collection, use or disclosure of your personal information. An opt-out option can be provided on the consent form.

Opt-out option – consent is also known as giving consent by not declining to give consent. This means that if you do not return a signed implied consent form then it will be considered that consent is granted.

Note: this will only be implemented for low to medium risk digital applications.

Express Consent – is used for when personal-sensitive information is collected or used. You give express consent if you give it openly and obviously, usually in writing. An organisation must get express consent before handling a person's sensitive information.

Why do we use online systems or digital applications?

Education in the twenty first century increasingly involves the use of online teaching and learning resources. All schools across the NT utilise digital applications as part of the modern curriculum and the digital applications are chosen to add value to a student's learning experience. Often these digital applications also allow the parent to view and interact with activities.

The Department of Education supports schools wanting to utilise digital applications by conducting assessments such as a security risk assessment. If the digital application or service captures personal or sensitive information, a Privacy Impact Assessment (PIA) is conducted, and a Privacy Information Statement (PIS) is prepared for assessed digital applications to help inform parent's decisions on providing consent.

Department of Education core digital applications

Department core digital applications enable the department to plan, provide and report on its services, and to monitor compliance under the *Education Act 2015*. These digital applications include but are not limited to Microsoft Office 365, One Drive, Email, Teams, SAMS G2, and SAIS.

What is Cloud computing?

Cloud computing is on-demand network access via the internet, to a shared pool of computing resources such as networks, servers, storage, applications, website hosting and services often hosted at a remote data centre. It allows for rapid access with minimal management effort or service provider interaction.

Online services – refers to any information and services provided over the internet. It includes all forms of externally provided or hosted digital applications or systems. This includes cloud computing services, most tablet and phone applications, and may also include some digital applications hosted inside the Department of Education ICT environment where the service provider is external and has access to records created in the digital application.

Data risk examples

The below table provides examples of types of student data and the level of risk associated to the different types of information.

Low Risk Data	Medium Risk Data	High Risk Data	Extreme Risk Data
Student School	Student name and year level	Student home address	Student medical records
Classroom details and schedule	Student or personal email	Student ID Card number	Student criminal records
Student attendance	Student images or videos	Student phone number	Credit card details
Formative assessments, for example polls or quizzes	Summative student assessment data	Custody details	Child abuse related information
		Indigenous status	Court orders
		Student parent relationship details	Witness protection

Further information

- For further information, talk to your school, or refer to the Department of Education website – https://education.nt.gov.au/policies/conduct
- NT Legislation includes Information Privacy Principles (IPPs) – https://infocomm.nt.gov.au/about-us/the-information-act
- Australian Government Office of the Australian Information Commissioner – https://www.oaic.gov.au/privacy/your-privacy-rights/more-privacy-rights/children-and-young-people
- https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/consent-to-the-handling-of-personal-information

Contact

Email rfi.doe@education.nt.gov.au for any concerns or further advice on privacy and consent.