POLICIES AND PROCEDURES

Privacy

KU Children's Services (KU) respects every individual's right to privacy and confidentiality. We openly and transparently manage personal and sensitive information of everyone at KU to support and enhance our role as an employer, provider and advocate for the safety, wellbeing, and development of children. The safety, rights and best interests of children is the organisation's paramount consideration.

INTRODUCTION

KU has access to personal information of children, families, employees, Board members, volunteers, contractors, consultants, visitors, donors, supporters, and alumni as part of providing high quality early childhood education and care services.

We are committed to processes and procedures for collecting, holding, using, disclosing and safeguarding personal and sensitive information in line with the requirements of the Australian Privacy Principles.

OBJECTIVES

KU Children's Services will:

1. Openly and transparently manage only personal and/or sensitive information which is reasonably necessary for KU to access in order to provide high quality early childhood education and care services.
2. Collect, hold, use and disclose personal and/or sensitive information of everyone at KU in accordance with the Australian Privacy Principles of the Privacy Act 1998 (Cth).
3. Ensure that everyone at KU understands we have processes and procedures in place to safeguard the privacy and confidentiality of their personal and/or sensitive information.
4. Regularly review and update as necessary the *KU Privacy Policy*, processes and procedures which respect and protect the privacy and confidentiality of personal and/or sensitive information.
5. Ensure stakeholders can freely and easily access this policy and information about how KU manages and safeguards their personal and/or sensitive information.

DEFINITIONS

Allow and deny listing: A process that allows access to trusted websites and applications while denying others.

Privacy

Continued...

Australian Privacy Principles (APPs): These form the cornerstone of privacy protection in Australia and govern the standards, rights and obligations around handling personal information (see summary on **page 17).**

APP Entity: An agency or organisation in Australia with an annual turnover of more than AUD $3M, which must comply with the Australian Privacy Principles (Schedule 1, Privacy Act 1988) governing the standards, rights and obligations around handling personal information.

Automated Decision Making (ADM): Refers to use of an individual's personal information by a computer program to make decisions which relate to and can be reasonably expected to affect the rights or interests of that individual; or to do something which is substantially and directly related to those decisions.

Children's Online Privacy (COP) Code: A set of rules the OAIC is mandated to develop by 10.12.26 to help keep children safe when using the Internet by ensuring organisations or companies that provide applications, websites and games safely use, protect and store personal information.

When it is finalised, the Code will set out specific requirements for how children's personal information should be handled online, ensuring that privacy protections for children in Australia are enhanced and that they comply with the Australian Privacy Principles (APPs).

Confidentiality: Refers to the duty to refrain from sharing an individual's personal information with others, except with the express consent of that individual, including:

- Something told in confidence, or in secret.
- The state of knowledge being held in confidence.
- The state of trusting another individual with one's private affairs or secrets.

Doxxing: Refers to the act of publicly and maliciously revealing personal or sensitive information online about individuals without their consent.

In the 2024 amendments to the Privacy Act 1988, doxxing was introduced as a criminal offence in the Criminal Code Act 1995.

Data Breach: Refers to situations of unauthorised access to, disclosure or loss of personal information held by an entity.

If a data breach is likely to cause serious harm to individuals affected, it becomes an 'Eligible Data Breach' under the Notifiable Data Breach (NDB) Scheme meaning that APP entities must notify both the OIAC and the individuals affected that a breach has occurred.

Eligible Data Breach Statement: Refers to a written notification providing details about an eligible data breach, the type of information involved, and recommendations for steps the individuals affected should take in response.

The organisation involved must use this statement to notify all affected individuals and the OAIC as soon as practicable.

OAIC: Office of the Australian Information Commissioner - the Independent national regulator for privacy and freedom of information, responsible for promoting and upholding personal rights to access government-held information and to have personal information protected.

Personal Information: Defined in Section 6 (1) of the Privacy Act 1988 (Cth) as information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- Whether the information or opinion is true or not.
- Whether the information is recorded in a material form or not.'

The Privacy and Personal Information Protection Act 1998, NSW also defines personal information as information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

Privacy takes different forms including:

- **Information Privacy:** Involves the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records. It is also known as 'data protection'.
- **Privacy of Communications:** Covers the security and privacy of mail, telephones, e-mail and other forms of communication.
- **Territorial Privacy:** Concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and ID checks.

  Ref: Report 108: For your information: Australian Privacy Law and Practice, Vol 1, May 2008 – Australian Law Reform Commission (ALRC) (Cth).

Sensitive Information: Defined in Section 6 (1) Privacy Act (1998), (Cth) as information or an opinion about an individual relating to their:

- Racial or ethnic origin.
- Political opinions or memberships.
- Religious or other beliefs.
- Professional, trade or union membership.
- Sexual orientation or practices.

- Criminal record.
- Health, genetic or biometric information.

Stakeholders: Refers to anyone at KU whose personal and/or sensitive information may be collected, held, used or disclosed by KU, including:

- Children and their families.
- KU Employees, Board members or volunteers.
- Consultants and contractors.
- Visitors, KU donors, supporters, and alumni.

IMPLEMENTATION

KU only collects, holds, uses and discloses the personal information of its stakeholders in ways that are reasonably necessary for the purposes of providing children and families with high quality early childhood education and care including therapy and supports and early childhood intervention programs.

KU will only use the personal of its stakeholders, for the reasons it was collected, or in ways that would be reasonably expected of a provider of services and NDIS programs in the early childhood education and care sector.

For example, to claim the Child Care Subsidy, KU is required to collect and disclose the personal information of families. We are also required to share this information in relation to NDIS audits. We will ensure that families involved in these situations are aware that we need to pass this information on to the Commonwealth Government.

It is also noted that as an advocate for the protection, wellbeing, and development of children in our care, circumstances may arise in which KU is required by law to provide personal information (including sensitive information) to another organisation. For example, where there are safety, welfare or wellbeing concerns for a child and reporting personal information to a 'prescribed body' or 'Information Sharing Entity' is mandatory.

KU will only disclose personal information to third parties if:

- It has consent of those involved.
- The disclosure is related to the primary purpose for which the information was collected and doing so would have been reasonably expected.
- It is legally obliged to disclose it.

What kinds of personal information does KU collect and hold?

KU's Privacy Policy (this policy), *KU's Code of Conduct* and *Standard Terms for the Enrolment of Children*, and legislative requirements concerning privacy and confidentiality, govern our management of personal information including family details for NDIS.

We are always prepared to discuss with families the reasons for requesting their personal information and any consequences of KU not being able to collect, hold, use or disclose such information – including circumstances where personal information is incomplete or inaccurate, and how that may affect KU's provision of services to children and families.

Anonymity

Wherever appropriate, KU gives individuals the option of remaining anonymous when communicating with KU. This will be most relevant where information is collected via the KU website and via survey.

In those cases, if information is collected that identifies the individual, we will de-identify it before storing or using it.

Third Party Privacy Policies

We may include or offer third party products or services as a necessary part of our delivery of early education services and training. These third parties have separate and independent privacy policies.

We require third parties to protect your information to the same degree that we do. Such third-party privacy policies are available upon request if you require more information.

The Right of Individuals to 'Opt Out' if They Do Not Wish KU to Use Their Personal Information

Donors and alumni are entitled to not have their names and financial gifts or contributions to KU (or KU Marcia Burgess Foundation) included on KU's donor recognition lists.

In addition, as a past child or a present or past family or staff member of KU, they have a right to not be sent updates and information about KU initiatives and events, KU alumni stories and benefits, and the KU Marcia Burgess Foundation.

KU Collects and Holds Personal Information

For children and families, this includes:

- Name, date of birth, and employment details.
- Address, home and mobile phone numbers and email addresses.
- Enrolment or attendance records

- Government-issued identifiers such as Medicare numbers, Centrelink Customer Reference numbers or NDIS plan details.
- Age, culture, family, and lifestyle.
- Court or Parenting Orders, Parenting Plans or contact arrangements with children.
- Family violence intervention orders protecting children's safety, welfare or wellbeing.
- Photos, images, and written records of children used in KU services to document children's learning and development; to display at services or for KU promotional material. We will only take and use photographs and artwork of children with authorised consent.
- Bank account and credit card details.
- Sensitive information, including medical conditions, health or medication needs, records of incidents, injuries or trauma, additional needs, and developmental assessments/reports including documentation from Allied Health and medical professionals provided by parents.
- Information about KU website users.

For KU employees, Board members, volunteers, consultants, contractors, donors, supporters, and alumni this includes:

- Date of birth, financial and superannuation account details, and tax file numbers.
- Name, address, landline, mobile phone number, and email address.
- Next of kin/emergency contact
- Copy of driver's licence or other ID (e.g. copy of passport).
- Biometric (e.g. use of fingerprint or facial recognition technology) to verify the identity of individuals.
- Court Orders.
- Salary and wage details.
- Medical (e.g. Workers Compensation, modified duties or personal leave, vaccination) records.
- Workers Compensation claims.
- Performance review and improvement documents and plans.
- Qualifications.
- Work rights verification, certifications, (e.g. Working with Children Check), copy of qualifications.

- NDIS Worker Clearance Checks where applicable.
- Cultural background information (e.g. Aboriginal and Torres Strait Islander).
- Information used to process financial donations, issue receipts and send updates.
- Supporter bequest intentions or other donor information outlining their needs or interests.
- Stories from past KU children, families, and staff about their KU experience and connection with the organisation including photographs and historical details (e.g. years of KU attendance) of their children, grandchildren and siblings.
- Training records/professional learning.

How does KU collect and hold personal information?

KU recognises the importance of having technical and organisational measures in place for securely collecting and storing personal or sensitive information so that it is protected from misuse, interference or loss.

We hold personal information on a secure electronic database maintained on a KU server or on the secure servers of cloud-based IT service providers engaged by KU.

Personal information regarding children attending allied health services is stored on an integrated cloud-based application.

KU's data storage processes ensure:

- Confidentiality and accuracy are maintained for all personal information, which is only accessible by persons authorised by KU or employees with an explicit need to know.
- Personal information recorded in paper form or by way of staff notes, will be digitised and/or kept safe and secure under restricted access at the service.
- KU employee records in KU Central Office under the management of KU's People Services and IT team are securely maintained.

KU's Commitment to Cyber Security

- KU implements cyber security measures which play an essential role in protecting the privacy and confidentiality of personal and sensitive information relating children, families, employees, volunteers and contractors at KU.

The KU Information, Technology and Communications (ITC) team provides the technical skills and experience to implement, protect, monitor, update, and maintain KU's ITC infrastructure and delivers technical support to everyone at KU.

The ITC team ensures our online services and devices are safeguarded by best practice cyber security technologies along with safe, legal and responsible user behaviour. This includes a commitment to only engaging reputable third-party support services as an essential layer of additional IT and communications security.

KU and the ITC team cultivate an organisation-wide culture of cyber resilience in response to current and evolving cyber threats and promotes understanding among everyone at KU of the types and levels of risk posed to early childhood education and care services by ITC security breaches, scams and attacks.

Data Breach Preparation and Response

KU recognises that under the Notifiable Data Breach Scheme (NDB) in Part IIIC of the Privacy Act 1988, it is required to notify the OAIC and any individual whose personal information held by KU has been compromised by a data breach.

A notifiable or 'eligible' data breach occurs when the following criteria are met:

- There is unauthorised access to, disclosure (e.g. doxxing) or loss of personal information.
- This is likely to result in serious harm to the individuals concerned.
- The likely risk of serious harm has not been prevented by remedial action.

In compliance with the NDB scheme, KU will respond to data breaches in the following steps:

1. Contain the data breach to prevent any further compromise of personal information.
2. Assess the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm.
3. Notify individuals and the Commissioner if required. If the breach is an 'eligible data breach' under the NDB scheme, it may be mandatory for the entity to notify.
4. Review the incident and consider actions to prevent future breaches.

Children's Online Privacy

We recognise that the health, safety, and wellbeing of children in our services is KU's highest priority as a provider of early childhood education and care, programs and early childhood intervention services.

We understand, therefore, the importance of providing learning environments which support children's developing digital literacies without compromising their physical or mental growth or ability to engage in play-based learning, build relationships and make social connections.

In anticipation of the OAIC's development of a Children's Online Privacy Code, KU will continue to maintain, monitor, and improve security and safety for children at KU in the way they access internet-based services including apps, websites, and messaging platforms.

Circumstances Which Allow the Release of Personal Information

The Education and Care Services National Regulations prescribe that information stored in records kept at KU education and care services relating to children, families, and staff must only be released in the following circumstances:

- If necessary for the education and care or medical treatment of a child to whom it relates.
- It will be provided to a parent (or person authorised by the family) of the child to whom the information relates (except in the case of information kept in a staff record).
- It is requested by the Regulatory Authority or an authorised officer.
- As authorised by an Act or law.
- If the person who provided the information has given permission for it to be released.

For children and families, we collect personal information in different ways, including:

- KU standard documents such as the *KU Enrolment Form* (including written or electronic methods) and the Family Details form.
- Email, written communications or notes from telephone conversations.
- Usage of KU website or Internet or direct enquiries about waiting lists.
- Educator observation reports and assessments of a child's development and behaviour.
- KU Allied Health observation, services and developmental reports.
- Educators and KU therapists taking photographs or video recordings of children at services.
- Information provided directly by family members, guardians, carers or persons authorised to do so on the family's behalf.
- Third parties (e.g. a health service provider) who have assessed or provided therapy for children who attend KU.
- Government agencies, advisors or family advocates who have dealt with families or people authorised to liaise with them on the family's behalf.
- A service provider engaged by KU or a third party who partners with KU.

Privacy

Continued...

For KU employees, we collect personal information via recruitment, induction, review and management processes during an individual's employment at KU including:

- KU standard forms.
- Usage of KU website or Internet and employee online platforms.
- Email, written communications, or telephone conversations.
- Productivity data/work performance records and related interactions.

For donors, supporters and alumni, we collect and hold personal information from donations made or written communications online or paper based.

The KU website collects statistical information only, which does not identify browsers or anyone who uses the site. This information may help us to improve navigation and engagement for visitors or to investigate market trends and preferences for the services we offer.

As the information we collect does not link to anyone's name, address or other identifier, we may disclose it to third parties to improve or develop the site and the user experience without breaching privacy or confidentiality requirements.

The website data KU collects includes:

- **Computer Address Information:** To enable communication between a visitor or user's computer and the server hosting this website, it is necessary that their web browser provides their computer's network address, including the top-level domain name (e.g. .com, .gov, .org, etc). In addition, the browser type and operating systems used may also be recorded.
- **Session, Navigation and Clickstream Data:** When anyone browses this website a trail of pages visited is generated as well as a record of the amount of data transferred and the date, time, and duration of access. It may also log the previous site visited by users. This information is recorded against the network address supplied by web browsers.
- **Cookies:** A cookie is a very small text file placed on a user's computer when they visit a website. "Session cookies" are used to make a website visit more effective, by temporarily storing a record of a user's navigation of the site. They are discarded at the end of the browsing session.

KU does not use cookies to identify anyone, connect identities with computer addresses or to track the navigational or browsing habits of identified visitors.

- Identifiable Personal Information
    - If a user emails KU via the website, only the information contained in their email will be collected (i.e. the content provided, including their email address).

- We will use the email address and its content only to reply to messages or supply you with the information or service you have requested.
- If we wish to use personal information to advise users about other KU services or opportunities, we will let you know what we propose to do and only do so with your consent.

As a provider of early childhood education and care and a NDIS registered provider, KU holds all records relating to children, families, and staff, in accordance with periods of time specified by regulatory requirements.

We keep your personal information only as long as required to provide you with products and services or employment and to comply with our legal obligations.

When the personal information we hold is no longer needed for these purposes, we take reasonable steps to destroy or permanently de-identify it.

The *KU Record Keeping relating to Children, Staff and Service Documents Policy* outlines the minimum timeframes that KU, as an approved provider, must hold different types of records, as prescribed by the Education and Care Services National Regulations.

Why does KU collect and hold personal information?

KU is committed to respecting and protecting the rights and interests of individuals in the way it manages personal information which is essential to its operations.

KU does not and will not use computer-based systems which use personal information to make automated decisions, especially those which can reasonably be expected to affect the rights or interests of anyone at KU.

KU collects, holds, uses, and discloses information for the purposes of:

- Providing children and families with education and care and early intervention services.
- Providing employment and fair working conditions to KU employees.
- Managing our relationship with children, families and employees.
- Complying with our legal obligations.
- Seeking funding in relation to our education and care services.
- Verifying Working With Children Checks (WWCC) in the areas of therapy/early intervention by collecting Driver's License details and/or dates of birth (DOB).
- Processing payments and tax receipts (e.g. to the Australian Government) for purposes of claiming the Child Care Subsidy or NDIS plan managers for the purpose of claiming NDIS funds.
- Partnerships or working with third parties.

- Performing functions and activities and operational processes.
- Managing and resolving complaints, allegations, incidents or issues.
- Managing risks.
- Conducting research, feedback, promotional or marketing activities.
- Creating donor lists which recognise the contributions of our financial supporters.
- Sending members of KU's alumni family updates and information about KU initiatives and events.

KU will not use or disclose personal information for any other purpose unless:

- Consent has been given by the stakeholder or parent/legal guardian if the information relates to children.
- We would be reasonably expected to use or disclose information related to children for another purpose which is directly related to our primary purpose.
- We are required or authorised by law and/or under the Privacy Act.

How can you access or correct your personal information held by KU?

KU takes every step to ensure the personal information of stakeholders we collect, hold, use, and disclose remains accurate, complete, up-to-date and relevant.

As a parent/guardian, you have a right to request access to your personal information, in accordance with the Education and Care Services National Regulations. There is no fee for making such a request.

If you are a parent/guardian, to assist KU with the process please:

- Contact the Privacy Officer (details below) who will assist you to access your personal information.
- In early childhood services and playgroups, if any of the personal information we hold about you is incorrect, incomplete or out of date, please inform the Director, Nominated Supervisor or Coordinator at your service.
- If any of the personal information we hold about you in allied health services is incorrect, incomplete or out of date, please inform your allied health therapist.
- If you are an employee, or any other stakeholder, please contact KU People Services and IT team directly to access or correct your personal information.

Special circumstances where KU is not required to provide access to your personal information or make corrections, include the following:

- KU believes providing such access would pose a serious threat to the life, health or safety of any individuals.
- Where there may be an unreasonable impact upon the privacy of other individuals.
- The request for access is frivolous or vexatious.
- The information relates to existing or anticipated legal proceedings.
- Giving access would be unlawful; or likely to prejudice an enforcement-related activity being conducted by an enforcement body.

Note: Where we decline access to or correction of your personal information, we will advise you of the reasons for this decision.

How can you give KU feedback or make a complaint about how we handle your personal information?

KU is committed to providing open, transparent, and responsive services and values feedback from children, families, Board members, employees, consultants, contractors, volunteers, visitors, donors, supporters, and alumni.

We will address any concerns or queries about how KU handles personal information:

- If you are a parent/guardian, volunteer, student or visitor please raise your concerns with the Director, Nominated Supervisor or Coordinator or Allied Health therapist at your KU service or program.
- If you are a Board member or employee, please contact the General Manager, People Services & IT.
- If you are a consultant or contractor, please contact your KU manager.
- If you are a donor, supporter or alumni member, please email KU at foundation@ku.com.au

Alternatively, if you are concerned about the way your personal information has been handled by the service or KU Central Office, you can contact the KU Privacy Officer (see below).

KU takes all complaints about privacy and confidentiality of personal information seriously.

If you are dissatisfied with the way your personal information has been managed by KU and wish to make a complaint about a breach of privacy, please contact our Privacy Officer (see contact details below).

- The first step is to lodge your complaint in writing.
- KU will consider and respond to a written complaint within a reasonable time.

- If your complaint remains unresolved, you may take your complaint to the Office of the Australian Information Commissioner (OAIC). See details below:
    - **Privacy Officer - KU Children's Services**
      Box Q132, QVB Post Office, NSW 1230

      Ph: 02 9264 8366

      Fax: 02 9267 6653

      Email: childrensservices@ku.com.au
    - **Office of the Australian Information Commissioner (OAIC):**

      Ph: 1300 363 992

      Fax: 02 6123 5145

      Website: www.oaic.gov.au

Is KU likely to disclose personal information to overseas recipients?

KU takes every step to ensure that information systems containing personal information are hosted locally within Australia.

If there is a requirement for a system to host personal information overseas, the following measures apply:

- A risk assessment must first be performed by the KU Information Technology and Communications (ITC) team and signed off by the KU Executive team.
- This risk assessment will thoroughly examine an overseas third party's privacy policy and whether it complies with relevant regulations. For example, the General Data Protection Regulation (EU) 2016/679 (GDPR) on data protection and privacy applies to organisations operating in member states of the European Union.
- KU will only engage overseas third parties to host KU systems if they are regulation compliant and potential risks to the organisation are assessed as low or minimal.
- KU will comply with any 'Allow and deny' listing developed by the Australian government identifying countries with acceptable privacy regulation standards.
- If it is likely KU will disclose personal information to overseas recipients, this policy will be updated as needed, to name the countries where such recipients are likely to be located, including those identified by the Government in its own listing when it becomes available.

Availability of This Policy

An online privacy statement summarising the *KU Privacy Policy* is available on the KU website (www.ku.com.au), including a link to this policy. KU will also make every effort to provide a copy of the policy in a format requested by any individual or interested party.

EVALUATION

This policy will be evaluated in line with KU's three (3) year policy review cycle, while ensuring it is up-to-date and reflects changing legislative requirements relating to privacy.

LEGISLATIVE APPLICATIONS

- Australian Professional Standards for Teachers
  - Standard 7.1, 7.2
- Child Safe Standards (ACT, NSW)
  - Standard 6, 8
- Child Safe Standards (VIC)
  - Standard 7, 9
- Children's Services Act 1996 (VIC)
  - Part 5D, Div 1-3
- Children's Services Act 1996 (VIC)
  - Part 5D, Div 1-3
- Children and Young Persons (Care and Protection) Act 1998 (NSW)
- Education and Care Services National Law
  - Section 175, 263, 264
- Education and Care Services National Regulations
  - Regulation168(2)(l), 177 (4), 177(4A), 177(4B), 181, 183
- Health Records Act 2001 (VIC)
- National Disability Insurance Scheme (Code of Conduct) Rules 2018
- National Disability Insurance Act 2013 (Cth)
- NDIS Practice Standards and Quality Indicators – Nov 2021 Ver. 4
- National Quality Standard
  - Standard 7.1.2

- National Principles for Child Safe Organisations
  - Principles 1, 2, 6, 7, 8
- Privacy Act 1988 (Cth)
  - Schedule 1: The Australian Privacy Principles
- Privacy and Other Legislation Amendment Act 2024
- Privacy and Personal Information Protection Act 1998 (NSW)

RESOURCES AND REFERENCES

- Early Childhood Australia Code of Ethics
- Protection of Personal Information – Information Sheet (ACECQA, July 2023)
- Data breach preparation and response – Guide to managing data breaches in accordance with the Privacy Act 1988 (Cth), July 2019
- Report 108: For your information: Aust Privacy Law and Practice, Vol 1, May 2008 – Australian Law Reform Commission (ALRC) (Cth)
- Office of the Australian Information Commissioner: www.oaic.gov.au
- NDIS Practice Standards and Quality Indicators No. 2021 Ver. 4
- For definition of confidentiality: www.legaldictionary.net/confidentiality

RELEVANT POLICIES

- Child Safe
- Code of Conduct
- ECI Service Agreements
- ECI Privacy and Confidentiality Statement
- ITC Acceptable Use of Assets and Services
- ITC Asset Management
- ITC Security
- ITC Software Evaluation
- Online Privacy
- Online Safety
- Record Keeping relating to Children, Staff and Service Documents
- Responding to Child Protection Complaints or Concerns involving KU Employees

- Responding to Child Wellbeing or Child Protection Concerns involving Vulnerable Children and Families
- Responding to Child Wellbeing or Child Protection Concerns
- Statement of Commitment to Cyber Security
- Standard Terms for Enrolment of Children

SUMMARY

The Australian Privacy Principles (APPs) form the cornerstone of Privacy Protection in Australia and govern the standards, rights and obligations around handling personal information.

These thirteen (13) principles are as follows:

1. **Open and Transparent Management of Personal Information**: Ensures APP entities manage personal information in an open and transparent way, including having a clear and up-to-date privacy policy.
2. **Anonymity and Pseudonymity:** Requires entities to give individuals the option of not identifying themselves or using a pseudonym, with some exceptions.
3. **Collection of Solicited Personal Information:** Outlines when entities can collect personal information that is solicited, with higher standards for sensitive information.
4. **Dealing with Unsolicited Personal Information:** Specifies how entities must handle unsolicited personal information.
5. **Notification of the Collection of Personal Information:** Details when and in what circumstances entities must inform individuals about the collection of their personal information.
6. **Use or Disclosure of Personal Information:** Defines the circumstances under which entities may use or disclose personal information.
7. **Direct Marketing:** Restricts the use or disclosure of personal information for direct marketing purposes unless certain conditions are met.
8. **Cross-border Disclosure of Personal Information:** Outlines the steps entities must take to protect personal information before disclosing it overseas.
9. **Adoption, Use, or Disclosure of Government-related Identifiers:** Limits the circumstances in which entities can adopt, use, or disclose government-related identifiers.

10. **Quality of Personal Information:** Requires entities to take reasonable steps to ensure the personal information they collect, use, or disclose is accurate, up-to-date, and complete.
11. **Security of Personal Information:** Mandates that entities take reasonable steps to protect personal information from misuse, interference, loss, and unauthorised access, modification, or disclosure.
12. **Access to Personal Information:** Outlines the obligations of entities when individuals request access to their personal information.
13. **Correction of Personal Information:** Details the obligations of entities to correct personal information they hold about individuals.

NEXT REVIEW

February 2029