Title: Privacy Management Policy

Purpose

The purpose of this Privacy Management Policy is to describe procedures for implementing a range of processes relating to the management of confidential information whether electronic or hard copy. This includes: file management, storage of staff diaries/workbooks, case notes, faxes, data base records, mail lists, and other records of interactions with children and young people and/or key stakeholders.

Policy Statement

CREATE is committed to ensuring that its Privacy Management system is accountable, open, and transparent. CREATE is committed to respecting children and young peoples' and carers' rights to privacy and confidentiality. All service users are entitled to access personal information that CREATE has on file about them and the right to make a complaint if they think information about them is not being handled properly.

Authority

Privacy Amendment (Enhancing Privacy Protection) Act 2012 Privacy Act 1988 (Commonwealth)

This policy sets out CREATE's internal strategy for complying with the Australian Privacy Principles (**APPs**), under the Privacy Amendment (Enhancing Privacy Protection) Act 2012, by:

- indicating which documents and materials produced by the organisation are presumptively open to CREATE representatives, children and young people, key stakeholders, and/or the public;
- indicating which documents and materials produced by the organisation are presumptively closed to CREATE representatives, children and young people, key stakeholders, and/or the public; and
- specifying the procedures whereby the open/closed status of documents and materials can be altered.

Definitions

Confidentiality: the principle that the circumstances of, or information related to individuals is private and its disclosure to a third party is limited and controlled.

Donor records: records pertaining to organisations/individuals who give funds to CREATE.

Electronic records: records kept on the organisation's information technology networks.

Hard copy records: paper based records such as printed emails, certificates, letters, case notes, reports, and registers.

Key stakeholders: all sector partners with whom CREATE has a relationship.

Personal information: information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and
(b) whether the information or opinion is recorded in a material form or not.

Privacy Officer**:** the CEO or delegated Manager responsible for matters relating to Privacy. The role is clearly identified within the organisation's Contact List that is circulated and available to all staff on Purple Pages.

Policy Approved by Board of Directors:	June 2015
Dates Reviewed:	Jun-18; Oct-21, Jul-24

Records: evidence of the interactions, activities, or transactions that occur when a service is provided to children and young people.
Sensitive information: information about a person's health, race, religion, or sexual preference.
Service users: children and young people aged 25 years and under who have a statutory care experience, and foster and kinship carers, and agency and residential care staff who access CREATE services, programs, and activities.
Volunteers: individuals who give their time freely to assist in the conduct of CREATE Foundation activities.

Categories
The following are categories used by CREATE to describe the types of records that they hold. Not all of these records contain "personal information" for the purposes of the Privacy Act:
Children and young people's records:

1. All child and young person's records shall be available to those individuals regardless of the child or young person's age;
2. No child or young person's record will be made available to anyone outside of the organisation if there is no duty to provide it (see the section on APP 12 below);
3. Within the organisation personal information relating to a child or young person is only accessible to those who need it to carry out their functions and obligations; and
4. There should be no occasion on which the Board would require access to confidential personal information held about children and young people. Non-identifying information can be made available to the Board.

Board records:

1. The Board operates in an open and transparent manner;
2. Board minutes may be requested, in writing; access to the minutes is at the discretion of the Board. Minutes will not be made available where the Board has passed a motion to make any specific portion of the minutes confidential;
3. If the Board denies any request, the Board will provide a written explanation for its refusal; and
4. The Company Secretary is responsible for maintaining company records and for responding to all requests for information from the Board.

Staff Records:

1. The Privacy Act does not classify staff-employment documents as personal information and therefore the Privacy Amendment (Enhancing Privacy Protection) Act 2012 does not apply to these records;
2. Individual staff records (HR files) shall be made available on request to the staff member concerned or to their legal representatives;
3. No staff records shall be made available to any person outside the organisation without authorisation in writing from the staff member concerned with the exception of providing the organisation's payroll provider with payment information; and
4. Within the organisation, staff records shall be made available only to those persons with managerial or personnel responsibilities for that particular staff member, except that staff records shall be made available to the Board and /or its legal representatives upon request.

Stakeholder and Donor records:

1. Individual stakeholder and donor records shall be available for consultation by the stakeholders and donors concerned or by their legal representatives;
2. No stakeholder or donor records shall be made available to any other person outside the organisation unless the disclosure is required by law; and
3. Within the organisation, stakeholder and donor records shall be made available only to those persons with delegated responsibility (i.e., with managerial or personnel responsibilities for dealing with those stakeholders and donors or the related accounts), except that stakeholder

and donor records shall be made available to the Board when requested by the Board.

Administrative records that do not contain personal information or employee records:

1. All records and materials not falling into the categories above (excluding such materials and records that contain personal information and employee records) may be released to the public at the discretion of the Privacy Officer, who shall take into consideration:

- a general presumption in favour of transparency;
- the relevant provisions of the Corporations Law regarding information to be made available to the public; and
- the marketing, commercial, legal, and administrative interests, priorities, and resources of the organisation, including:
    - commercial confidentiality; and
    - copyright issues.

COMPLIANCE WITH THE AUSTRALIAN PRIVACY PRINCIPLES

APP 1: Open and transparent management of personal information

1 Requirements

APP 1 requires organisations to have ongoing practices and policies in place to ensure the management of information in an open and transparent way.

The first part of compliance with this requirement is to have a compliant privacy policy. It also requires organisations to take "reasonable steps in the circumstances" to implement practices and procedures for dealing with personal information, and to explain to service users and stakeholders what these are. Compliance with this requirement requires a comprehensive analysis of what personal information an organisation collects or receives, when it is disclosed, and how it is used.

2 Compliance strategy

CREATE has an internal set of policies and procedures for the effective management of information addressed in this privacy management policy. CREATE also has a privacy statement aimed at the public which covers how CREATE deals with personal information. CREATE reviews these documents regularly and updates them where necessary to keep them compliant with the APPs.

Further, all CREATE staff and volunteers are informed of the confidentiality and privacy requirements in CREATE's policies and procedures. All staff and volunteers are required to sign a Confidentiality Agreement stating that they will keep confidential all information that they deal with, unless there is a valid reason for disclosure that is permitted by law. The delegated HR Officer is responsible for filing the signed Confidentiality Agreement in an individual's personnel record.

All CREATE staff and volunteers are required to participate in privacy training, where relevant.

APP 2: Anonymity and Pseudonymity

1 Requirements

APP 2 requires organisations to give individuals the option of dealing with the organisation using a pseudonym, unless it is impractical to do so, or if the organisation is required by law to identify an individual. Guidance issued by the Privacy Commissioner to date indicates that this APP will also require organisations to make individuals aware of their option of dealing anonymously or through a pseudonym, and to inform individuals of any disadvantages of doing this.

2 Compliance strategy

In many situations it may not be practicable for CREATE to allow service users to use a pseudonym or operate anonymously, as it cannot provide services or programs to individuals if users are not identified.

Where CREATE deems that it is practicable to deal with an individual either anonymously or pseudonymously, e.g., in collecting non-identifiable research data, CREATE will inform the individual concerned that they have the right to deal anonymously or pseudonymously with CREATE. This may happen either via a notification on a webpage (where the information is collected via the internet as in surveys, or research), or before CREATE staff begin face-to-face or telephone interviews where personal disclosures may be made.

APP 3: Collection of solicited personal information

1 Requirements

APP 3 sets out how personal information may be collected. It requires that an organisation must only collect personal information that is reasonably necessary for the organisation's functions and activities. Information must only be collected from the relevant individual unless it is unreasonable or impractical to do so.

To comply with this requirement, organisations need to review the requests they make for information from individuals (e.g., when applying for membership) to determine if they are reasonable. For example, it is reasonable to ask for a date of birth if it is required to verify age, but it may not always be reasonable to require information on the demographics of their family.

There are also additional restrictions on the collection of any sensitive information (e.g., information about a person's health, race, religion, or sexual preference) which may generally only be collected with consent and if it is reasonably necessary to do so.

2 Compliance strategy

The CREATE Foundation collects personal information only when it is essential for it to carry out its functions or activities prescribed in funding and/or Service Agreements.

There are times, however, where CREATE requires personal information in order to effectively provide services to individuals. For example, when an individual applies for a *clubCREATE* membership, CREATE requests the following information:

- full name;
- address;
- email address;
- phone number;
- date of birth;
- sex;
- cultural status;
- care type;
- carer's details (optional if the young person is over 18 years of age); and
- caseworker's details

The other types of personal information that CREATE might collect for specific events or projects include:

- medical information;
- next of kin;
- behaviour;

- statistical information (numbers of children attending programs, functions, events and so on);
- carer / volunteer personal and demographic details;
- file notes regarding individuals;
- correspondence between service users and/or donors and CREATE;
- reports regarding individuals;
- training records; and
- information for research purposes.

CREATE collects a variety of sensitive information. If a CREATE staff member or volunteer believes that it is necessary to collect sensitive information to provide services to an individual, the staff member needs to first ensure they are following organisational policy and have the consent of the person before attempting to collect that information. The date, time, and medium of consent (e.g., in writing, in person, over the phone) should be recorded against the sensitive information as an indicator that consent was given.

If a child or young person discloses sensitive information relating to abuse and/or neglect CREATE staff will follow the process outlined in the Protecting Children Policy.

APP 4: Dealing with unsolicited personal information

1 Requirements

APP 4 specifies how an organisation must deal with personal information that it has received unsolicited. Within a reasonable period of receiving the information, the organisation must assess whether it could have collected the information under APP 3, and if not must destroy or de-identify the information.

Organisations need to have a process for dealing with information that they have not requested, such as emailed enquiries containing unnecessary personal details, or unsolicited employment applications.

2 Compliance strategy

CREATE may receive unsolicited information:

(a) through general email and telephone enquiries, working with sector partners, and as a consequence of specific complaints;
(b) during CREATE events and activities; and
(c) in employment applications.

CREATE's general policy is that unsolicited personal information should not be recorded if the information is clearly not necessary for CREATE to perform its services.

If an employee or volunteer is unsure of whether or not information is relevant, the employee must record that information. Once the information has been received, the staff member must discuss with their supervisors, or if necessary, with the CREATE Privacy Officer, whether or not the information should be retained. If it is determined that the information is not relevant or should otherwise not have been collected, it must be destroyed.

APP 5: Notification of the collection of personal information

1 Requirements

APP 5 sets out matters that an organisation must inform individuals of at the time their personal information is collected. These include:

- what information is being collected and the purposes for which it is used;

- the contact details of the collecting entity;
- the consequences to the individual of choosing not to provide any information;
- how the individual may access the information or request that it be corrected;
- the types of bodies or organisations that the information may be disclosed to, and if the information may be disclosed overseas, the countries to which it is likely to be sent; and
- how the individual can make a complaint about the use of their personal information.

For example, if an organisation is conducting market research, the caller needs to inform the individual of these things at the start of each call.

2 Compliance strategy

CREATE must ensure that the individuals on whom CREATE holds personal information are aware that the information is held and understand the purpose of collection and the circumstances in which information can be used and disclosed. CREATE must also notify individuals how they can access the collected information and what the relevant procedures are if they wanted to lodge a complaint concerning the information. Where possible, CREATE will notify the individuals of these facts at the time the personal information is collected. The particular notification given to each individual may vary in accordance with the type of personal information being disclosed and the purpose for which it is being disclosed.

To this end, CREATE has inserted the following statement on webpages where personal information is collected and on CREATE collateral:

Privacy and your personal information
Your personal information is protected by the Privacy Act 1988 and the Privacy Amendment (Enhancing Privacy Protection) Act 2012. We will only use the information that you give to us to provide our services to you. We may disclose the information that you provide to third parties who assist us in providing our services to you, or if we are required to do so by law.

For further information about how we manage your personal information, how you might update or access your information, or to make a compliant, please view our policy at: http://create.org.au/privacy-policy/

When CREATE collects personal information over the phone, the operator must provide the individual with a verbal collection statement. The standard CREATE collection statement given over the phone is:

We will only use the information that you give us to provide our services to you. We may disclose the information that you provide to third parties who assist us in providing our services to you, or if we are required to do so by law. If you do not provide us with the information we request, we may not be able to provide our services to you.

For further information about how we collect, use, dispose of, and disclose your personal information, please refer to our Privacy Policy, available online. Our Privacy Policy also explains how you can access the personal information we hold about you and what you need to do if it needs to be updated.

CREATE also provides similar statements at the commencement of surveys that are used to collect data for research/consultation purposes. These statements are specific to the particular research project and subject to ethical clearance.
Further, CREATE informs individuals of the Privacy Management Policy and the Complaints Policy via:

- *clubCREATE* magazines;

- CREATE website;
- Young Consultants Training;
- Youth Advisory Group meetings;
- promotional and marketing material; and
- direct service provision.

CREATE staff members must ensure that they also inform individuals that CREATE's Privacy Officer acts as the first point of contact for privacy issues that may arise. The Privacy Officer is responsible for responding to the query in a timely manner (within 10 working days) and determining whether the issues raised in relation to records management are a process issue or should be handled as a complaint (refer to the Complaints Policy for guidelines.)

APP 6: Use and disclosure of personal information

1 Requirements

APP 6 regulates how an organisation may use and disclose personal information that it holds. Generally, information may only be used for the purpose for which it was collected, or a related secondary purpose unless consent for further use has been given by the relevant individual.

For example, an organisation may use information that it collected from account holders to provide them with a new service. However, the organisation may not give that information to a related company to provide a different service unless it has sought permission from the individual to do so.

2 Compliance strategy

(A) Use of personal information

Personal information should only be used for the purpose for which it is collected. Any proposed exception to this principle must be approved by the CEO or Privacy Officer before being implemented. In assessing any request to use personal information for a secondary purpose, the CEO or Privacy Officer must consider if this is permitted under the Privacy Act. Generally, the information may be used for a secondary purpose if that secondary purpose is sufficiently related to the primary purpose, such that the individual could have expected the information to also be used for that purpose. If necessary, additional consents may be sought from relevant individuals.

Where service user statistical data are collected, it is to be coded using either an alpha code or client number, but not using the client's name. CREATE may use service user statistical data for research purposes.

CREATE will take reasonable steps to destroy, archive, or permanently de-identify (white out, block out with marker) personal information if it is no longer needed.

(B) Applications for employment/volunteer work

CREATE may receive applications for employment which are in response to an advertisement for a specific position, or which are made as general expressions of interest.

Where applications are received for a specific advertised position, the application must only be used to assess the candidate's suitability for that position, unless the candidate has also requested that the details be kept as a general expression of interest for other positions.

If an applicant has made a general expression of interest, their details may be used to

assess their suitability for multiple positions.

If an application for employment is successful, the information gathered during the recruitment process is no longer personal information covered by the Privacy Act 1988, but becomes an employee record.

(C) Disclosure

Any information held by CREATE is generally not to be shared or provided to a third party without express permission from the individual, and if applicable, the statutory body in the State in which the individual is in care. Notwithstanding this, CREATE has a duty of care obligation to report child protection concerns, and to pass relevant data or evidence, if appropriate, to statutory bodies or the Police (refer to subpoena request section below in APP 12 for more information.)

(D) Photos

Children and young people must not be identifiable in photographic images, or have their full name used in any publication or material produced by CREATE without the express permission of the statutory body (in writing) in the state where the child is in care (unless the young person is over the age of 18 years).

In addition to the Privacy Act requirement, it is generally not permitted to identify any child under the age of 18 years of age as being in the care of the State unless CREATE has express permission from the relevant statutory body in writing and with the approval of the Privacy Officer.

Photographs of children and young people under the age of 18 years must not be displayed by CREATE in state offices where the public have access or in any publications.

(E) Life stories, narratives and life histories

Children and young people's stories, narratives, life histories, and personal experiences cannot be shared or published in the public domain without their express approval. This includes children and young people of all ages. It is not permissible merely to change the child's name to protect their identity. If any aspects of the information disclosed could reasonably identify the child, a witness, or an offender, CREATE must either delete or remove those identifying elements from the life story, or not disclose the life story at all. Life stories are deeply personal and should be respected.

(F) clubCREATE

A major component of C*lubCREATE* is an electronic database that records service user information for the purpose of registering membership of the club to facilitate the distribution of the clubCREATE magazine and other information about activities. *ClubCREATE* data cannot be provided to a third party without approval from the CEO and written approval from any relevant statutory funding body where appropriate.

CREATE will not disclose personal information about any individual to others in the absence of a legal obligation to provide it, unless it is deemed to be in the service users best interest in accordance with state legislation which includes any mandatory reporting obligations.

(G) Sortli App

The Sortli App is to assist young people aged from 15 to 17 years old with their transition from out-of-home care to independence. CREATE collects de-identified usage data including when

and how the app is used, pages accessed, types of functions used, number of users. Information entered into the Sortli app (e.g. ~~your~~ budgets and expenses) is stored locally on the users device, and not accessed by CREATE. If feedback is provided ~~on~~ https://create.org.au/privacy-policy/ the Sortli app, email address and any other information shared with us will be collected and handled in accordance with this policy.

APP 7: Direct marketing

1 Requirements

APP 7 regulates the use of personal information for direct marketing. Generally, use of personal information for direct marketing is only permitted where the individual has given their consent to the marketing, or where their information has been collected in circumstances where the individual could reasonably expect that the information would be used in this way.

For example, if an organisation collects information from a person when the person opens an account, the individual may reasonably expect that the organisation may email them about their account, or products used in their account. However, if the organisation wishes to use the person's contact details to advertise unrelated products, it will generally need to obtain the individual's consent.

2 Compliance strategy

(A) Opt in customers only

It is CREATE's policy to send direct marketing notifications only to consumers who have opted to receive them. Notifications should not be sent to any consumers who have not elected to receive the marketing material.

(B) Unsubscribe notices

The following text is one example that can be displayed at the base of all marketing material, to ensure that consumers have the opportunity to opt out at any time:

*You are receiving this message because you have opted to receive marketing notifications from CREATE. If you no longer wish to receive these emails, please [click here: **Unsubscribe**/write to us at [insert email address]].*

Once a consumer has elected to unsubscribe from marketing material, that individual must be removed from CREATE's recipient list immediately.

APP 8: Cross-border disclosure

1 Requirements

APP 8 regulates the transfer of personal information from Australia to other countries and introduces a greater level of accountability for Australian organisations that transfer information overseas. This accountability cannot be removed, and risks should be mitigated with appropriate provisions in supplier contracts, and technical assessments of the ability of overseas suppliers to keep information secure.

For example, if an organisation has engaged a third party to provide hosting of customer data outside of Australia, it is important that it have done due diligence to ensure that the third party is technically in a position to keep that data secure. The organisation's agreement with the third party should also require it to use appropriate measures to keep the customer data secure, and to comply with the APPs.

2 Compliance strategy

CREATE does not transfer any personal information held to any country outside of Australia. If this situation changes, the privacy policy and collection statements will be updated to identify each country from which, or to which, personal information is accessible or transferred. The exception to this is when CREATE staff travel overseas and access CREATE information whilst in another country.

If CREATE considers engaging any service providers in the future who may access personal information from outside Australia or transfer it outside of Australia, CREATE will consider the legal position of individuals in that jurisdiction, and what protections and remedies would be available if the information were disclosed, before making the decision to engage that service provider.

In particular, CREATE will need to consider its statutory and regulatory obligations in relation to cross- border disclosures of sensitive data relating to children and young persons in care. Sensitive data of this type may be subject to restrictions on cross-border disclosures.

CREATE will also update its Privacy Management Policy to reflect any changes in this regard.

APP 9: Adoption, use, or disclosure of government related identifiers

1 Requirements

APP 9 prohibits an organisation from adopting a government identifier unless required by law (such as a tax file number) or disclosing a government identifier unless an exception applies.

2 Compliance strategy

As a matter of policy, CREATE does not use government identifiers to identify an individual.

APP 10: Quality of personal information

1 Requirements

APP 10 requires an organisation to take reasonable steps to ensure the personal information it collects is accurate, up to date, and complete. This requires organisations to take actions such as requesting current account holders to update their details from time to time but does not require that personal information that is not being used (e.g., from accounts that have been closed) is updated.

2 Compliance strategy

CREATE uses several different procedures to ensure that consumer information that it holds is up-to-date and as accurate as possible. These procedures include:

(a) Sending notifications to consumers who receive marketing material from CREATE to remind them to review and update their details;
(b) Prompting consumers who contact CREATE to update their details; and
(c) Notifying consumers for whom CREATE receives an “undeliverable” message in response to an email or postal communication, if another form of contact is possible, that their address details appear incorrect and need updating,

CREATE may retain data from unsuccessful job interview candidates. CREATE seeks consent from the candidate at interview asking if they would like to be considered for future positions. This material is maintained for a maximum of six months. Data provided by unsuccessful applicants is destroyed at the completion of the recruitment process.

If the individual and the organisation disagree about whether any information is accurate, complete, and up-to-date, the person making the request can ask that the organisation place additional information on the file. This can be done via a written statement claiming that the

information is not accurate, complete, or up-to-date and explain what needs to be corrected and why. CREATE will take reasonable steps to include all relevant information on the individual's file.

APP 11: Security of personal information

1 Requirements

APP 11 requires an organisation take reasonable steps to protect the personal information it holds against interference, misuse, or loss, or unauthorised access, modification, or disclosure. The steps required to protect the information are relative to the type of information and its sensitivity to the relevant individual.

The standard of required security depends on the type of information and what is reasonable in the circumstances. For example, payment information requires a higher standard of protection than a list of email addresses.

2 Compliance strategy

(A) Limitations on access to information

CREATE only provides access to personal information it holds on a need to know basis. This means that:

(a) only HR or delegated staff with a need to know may access responses to advertisements for vacant employment opportunities;
(b) all HR or delegated staff may access resumes when the applicant has requested their resume be kept on file as an expression of interest, but no other part of the business can access these files;
(c) only relevant finance staff are permitted access to payment information; and
(d) only the delegated staff are permitted access to information on service users.

(B) Physical security of records

All printed personal information is to be stored in secured cabinets and only accessible to staff who need the information to carry out their duties.

To prevent unlawful access to personal and/or sensitive information, all records including files should not be left unattended in the office (including in-trays). Information should be locked away when not in use. Unauthorised persons should not be allowed entry into confidential work areas.

CREATE will store data in secure locations in either hard copy or electronic formats. Staff computers must be locked and only accessible by password when not in use or unattended for any period of time.

The *ClubCREATE* database may only be accessed by staff nominated by the Privacy Officer, and is password activated.
Hard copy service-user files should not be transported out of the office, unless in extenuating circumstances and approved by the CEO or delegate Privacy Officer. Security measures appropriate to the format of the information must be put in place. For example, if records need to be transported, the person transporting the records should ensure they are secure. It is the responsibility of the Privacy Officer to supervise the security of user files. If any staff member or volunteer has a query in this regard, they must raise it with the Privacy Officer.

All information disposed of by CREATE containing identifying information must be shredded by either placing the information in the appropriate safe destruction bins on site, or by directly shredding the information in the document shredders on site.

No hard copy personal information or records of service users can be held off-site, and remote access to information held on CREATE systems is only available in extenuating circumstances to delegated staff authorised by the CEO. For example, at some off-site activities (such as camps) it is necessary to have personal information at hand to ensure the safety and wellbeing of children and young people. Approval for such access must be obtained from the Privacy Officer in writing before the event is conducted.

Hard copy staff diaries and case notes are an official and legal record, and accordingly need to be treated with care as outlined below:

- used staff diaries containing private or confidential information about children and young people should be stored and filed in locked and secure archive storage for 7 years. State Coordinators are responsible for ensuring that diaries are returned by staff and stored.
- current staff diaries should be stored securely if they contain confidential client information. Staff should ensure that contact details, and full names of children and young people are NOT included in their diaries. For example, the first name OR surname may be used but NOT the full-name.

(C) Specific requirements for files on children/young people/carers

CREATE generally does not hold files on children and young people or carers. However, in circumstances when they do, the following process should be adhered to:

(a) Any files regarding carers and children and young people are to be located in locked filing cabinets in each state and/or territory;
(b) The files are to be locked each evening and the key located in a secure (locked) location;
(c) Computer files holding personal information of service users are only available to staff in the state in which they reside; and
(d) Confidential files on carers and children and young people that are inactive for 2 years are to be stored by CREATE in archive files for 7 years, and then where appropriate (dependent on state legislative requirements) forwarded to the statutory body in each state and / or territory. This is the responsibility of State Coordinators.

APP 12: Access to personal information

1 Requirements

APP 12 requires organisations to give individuals access to the personal information that the organisation holds about the individual unless an exception applies. The following exceptions may release the organisation from providing access under the Act:

- The organisation reasonably believes that giving access would pose a serious threat to the life, health, or safety of any individual, or to public health or public safety (APP 12.3(a));
- Giving access would have an unreasonable impact on the privacy of other individuals (APP 12.3(b));
- The request for access is frivolous or vexatious (APP 12.3(c));
- The information relates to existing or anticipated legal proceedings between the organisation and the individual, and would not be accessible by the process of discovery in those proceedings (APP 12.3(d));
- Giving access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations (APP 12.3(e));
- Giving access would be unlawful (APP 12.3(f));
- Denying access is required or authorised by or under an Australian law or a court/tribunal order (APP 12.3(g));

- The organisation has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the organisation's functions or activities has been, is being, or may be engaged in, and giving access would be likely to prejudice the taking of appropriate action in relation to the matter (APP 12.3(h));
- Giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body (APP 12.3(i)); and
- Giving access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process (APP 12.3(j)).

If none of the exceptions apply, the organisation must give the individual access. A reasonable charge may be applied for the cost of providing access.

To comply with this requirement, organisations need to respond to requests from individuals to give access to their information, and to inform them up front of any fees. There must be a consistent process for treating similar requests in the same way.

2 Compliance strategy

CREATE is not covered under the Freedom of Information Act as it is a non-government organisation. CREATE's information is released under an "Administrative Release" framework and will provide individuals with access to their personal information upon written request if deemed appropriate. Administrative Release is a term commonly used in the non-profit sector to identify the terms under which documents can be released. There is no charge for this service.

Personal information held on file by CREATE may be accessed by the following:

- the individual about whom information is stored (upon written request);
- the court through subpoenas requesting documents; and
- the statutory funding body (in each state and/or territory).

If service users wish to have access to information that CREATE holds about them, they need to formally advise CREATE in writing of their request. If service users make their requests in any other way, CREATE must inform the service users that their requests are to be made in writing.

If CREATE determines for any reason (as listed in the exceptions above) to deny access to the information, it will provide reasons for denying access in writing within 14 days of receipt of the request. This should be done after consultation with and approval from the CEO.

CREATE requires a minimum of 15 working days and a maximum of 30 days to process written requests for the release of information. Every effort will be made to release information within the 15-day period.
If CREATE anticipates that this deadline cannot be met, the CEO should be notified, and the person making the request will be informed and a new date negotiated.

APP 13: Correction of personal information

1 Requirements

APP 13 requires an organisation to correct personal information to ensure that it is accurate, up-to-date, and not misleading if either the organisation is satisfied that the information needs to be corrected, or if individuals request that their information be corrected. If information that has been corrected has been given to another company, the organisation generally is required to inform the other company of the correction.

2 Compliance strategy

If an individual requests that CREATE update or correct information that CREATE holds about the individual, CREATE will do so, as long as:

(a) CREATE is able to identify the individual; and

(b) CREATE does not reasonably believe that the information CREATE holds is correct.

If CREATE refuses to correct personal information, CREATE will give written reasons to the individual for refusing to correct the information.

If CREATE receives information from a third party which CREATE subsequently determines is incorrect, CREATE must promptly inform the third party of the error.

If CREATE discovers that information it has given to a third party is not correct, CREATE will promptly contact that third party to correct the error.

Links

- Child Protection Practice Guide
- Complaints and Feedback Policy
- Confidentiality Agreement
- Consultation with Children and Young People Policy
- Information Security and Data Management Policy
- Information Technology Policy
- Risk Management Policy