Title: Privacy Management Policy

PART A: BACKGROUND

Policy Statement

CREATE is committed to ensuring that its Privacy Management system is accountable, open and transparent. CREATE is committed to 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 Act 1988 (Commonwealth)

Links

Complaints and Feedback 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 transactions for service users and / or key stakeholders.

The purpose of this policy is to set out CREATE's internal strategy for complying with the Australian Privacy Principles (**APPs**) under the Privacy Act 1988, including to:

- indicate which documents and materials produced by the organisation are presumptively open to members and/or the public;
- indicate which documents and materials produced by the organisation are presumptively closed to members and/or the public; and
- specify the procedures whereby the open/closed status of documents and materials can be altered.

Definitions

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.

Service users – includes children and young people under the age of 25 years that have a care experience, and foster and kinship carers and / or grandparents who access CREATE services, programs, activities, and newsletters.

Key stakeholders - all relationships that CREATE has with sector partners, including those who may hold CREATE membership.

Records - are the evidence of the transactions or activities when providing a service to service users, consumers.

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

Electronic records – computer based records kept on the agencies computer system.

Privacy Officer – is the delegated CREATE Manager responsible for matters relating to Privacy

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:

1. All children and young peoples' 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. Upon written request, Board minutes may be viewed at the discretion of the Board. This excludes 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 their 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. Staff records are not personal information and therefore the Privacy Act 1988 does not apply to these records. However, CREATE has chosen to make certain records available to staff regardless;
2. All staff records (HR files) shall be available 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; 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 when requested by the Board.

Member and Donor records:

1. All member and donor records shall be available for consultation by the members and donors concerned or by their legal representatives;
2. No member 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, member and donor records shall be made available only to those persons with managerial or personnel responsibilities for dealing with those members and donors or the related accounts, except that member 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 (Operations Manager), who shall take into consideration:
   - a general presumption in favour of transparency;
   - the relevant provisions of Corporations Law regarding information to be made available to members; and
   - the marketing, commercial, legal, and administrative interests, priorities, and resources of the organisation, including:
     - commercial confidentiality; and
     - copyright issues.

PART B: 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 customers 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 policy 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 up-to-date and 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 signed Confidentiality Agreement is then filed in individual personnel files by HR or the delegated Officer.

All CREATE staff and volunteers are required to participation 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

At all times, CREATE staff members and volunteers need to consider whether CREATE needs to deal with individuals using their real names in order for it to run its services. If it is not necessary, CREATE should give the individual concerned the option of dealing with CREATE anonymously or through a pseudonym.

For example, when a child or young person joins clubCREATE, CREATE normally asks the child or young person for the name of their carer. In this situation, as this information is not necessary for CREATE to provide its services to the individual, CREATE must inform the individual that they are not required to give that information.

However, in some situations, it may not be practicable for CREATE to give that option to the people using its services. For example, it may not be advisable for CREATE to allow volunteers who work with service users (for example, in running seminars and activities for children and young persons) to use a pseudonym or to deal anonymously with CREATE. Similarly, it may not be practicable for CREATE to allow service users to use a pseudonym or operate anonymously.

Where CREATE deems that it is practicable to deal with an individual either anonymously or pseudonymously, CREATE either:

(a) where the information is collected via a webpage, informs the individual concerned that they have the right to deal anonymously or pseudonymously with CREATE via a notification on that webpage; or

(b) where the information is collected over the phone, informs the caller of their right to deal anonymously or pseudonymously with CREATE, either before or as soon as practicable after they disclose any personal information.

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 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 does not collect personal information unless the information is essential for it to carry out its functions or activities outlined 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:

- name;
- address;
- email address;
- phone number;
- carer's name (optional); and
- information collected for research purposes (link to anonymous info).

The other types of personal information that CREATE may collect includes:

- 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
- research.

As a general rule, CREATE does not collect 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 have the consent of the person before collecting that information. The date, time and medium of consent (eg. in writing, in person, over the phone) should be recorded against the sensitive information as a record that consent was given. The staff member or volunteer must then check with their supervisor or the CREATE Privacy Officer if the sensitive information is required or not. If the supervisor or privacy officer deems that the information is not required, that sensitive information must be destroyed.

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 and 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 call is over, the operator must discuss with their supervisor, 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.

CREATE's standard policy is that all sensitive information should be destroyed, unless an exceptional circumstance requires it to be kept.

APP 5: Notification of the collection of personal information

1 Requirements

APP 5 sets out matters which 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, can be accessed, the purpose of collection and the circumstances in which information can be used and disclosed. CREATE must also notify individuals on the relevant complaint procedures. Where possible, CREATE notifies 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 collection statements on webpages where personal information is collected. When CREATE collects personal information over the phone, the operator must provide the individual with a verbal collection statement. The standard CREATE collection statement to give over the phone is:

"*We will only use the information that you provide to us to provide our services to you. We may occasionally 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 and disclose your personal information, please refer to our Privacy Policy, available online. Our Privacy Policy also explains our complaint procedures, how you can access the personal information we hold about you and ask us to correct it."

Further, CREATE informs individuals of the Privacy Management Policy and the Complaints Policy via:

- ClubCREATE newsletter;
- CREATE website;
- Young Consultants Training;
- Youth Advisory Council Training;
- promotional and marketing material; and
- during direct service activities.

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.

APP6: Use and disclosure of personal information

1 Requirements

APP6 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 which it collected from account holders to provide them with a new service. However, the organisation may not be able to 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. If a staff member wishes to use information for any secondary purpose, this must be approved by the Privacy Officer first. In assessing any request to use personal information for a secondary purpose, the 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 would 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 is collected, it is to be in code format (either alpha code or client number) and 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.

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 their details be kept as a general expression of interest.

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.

a. 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 subsequent data, or evidence if appropriate, to statutory bodies or the Police. Refer to subpoena request section below in APP 12 for more information.

Release guidelines – Subpoena request
If personal information held by CREATE is the subject of a subpoena request:

1. All information listed on the subpoena is to be released;
2. All references to other parties (other children in care, or other people not identified on the subpoena) are to be deleted. If the scope of the subpoena includes other parties this must be complied with;
3. If staff are unsure of the requirements, queries for clarification should be directed to the authority requesting the subpoena; and
4. The CEO or delegated Manager is responsible for authorising information to be released for subpoenas.

Photos:

Children and young people must not be identified by photographic image, or by full name 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 child or 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 as being in the care of the State.

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.

Life stories, narratives and life histories:

Children and young people's stories, narrative, life history 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.

clubCREATE:

clubCREATE is an electronic data base that records consumer (children, young people and foster carers) information for the purpose of membership to the clubCREATE newsletter and other information and activities.

clubCREATE data cannot be provided to a third party without written approval from a statutory funding body and approval from the CEO.

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

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 would 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

Opt in customers only

It is CREATE's policy to only send direct marketing notifications 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.

Unsubscribe notices

The following text is 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, but 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

The personal information held by CREATE is not transferred to, or accessible from, any country outside of Australia. If this changes, the privacy policy and collection statements will be updated to set out each country from which, or to which, personal information is accessible or transferred.

If CREATE considers engaging any service providers in the future who may access personal information outside of 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 was 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 policy and 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.

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 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 regular notifications to consumers who have 'opted in' to receive marketing material from CREATE to remind them to review and update their details;
(b) where a consumer calls CREATE, prompting the consumer to update their details; and
(c) if CREATE receives an 'undeliverable' message in response to an email or postal communication to a consumer, sending the individual a notification by other means where possible to prompt that individual to update their details.

If CREATE retains unsuccessful or speculative job applications on file to match them with future suitable jobs, CREATE must take steps to ensure the information in the application is up-to-date. For example, CREATE should regularly contact applicants to request that they verify that their application is up-to-date. CREATE only retains unsuccessful or speculative job applications on file for a maximum of two years.

If the individual and the organisation disagree about whether the 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 add, or include the 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

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 staff with a need to know may access responses to advertisements for vacant employment opportunities;
(b) all HR 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.

Physical security

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

To prevent unlawful access 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 CEO, and is password activated.

Service user files should not be transported out of the office, unless in extenuating circumstances and approved by the Privacy Officer or CEO. Security measures appropriate to the format of the information must be put in place. For example, if records are required 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 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.

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.

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

1. Any files for carers and children and young people are to be located in locked filing cabinets in each state and/or territory;
2. The files are to be locked each evening and the key located in a secure (locked) location;
3. Computer files holding personal information of service users are only available to staff in the state they originate from; and
4. Confidential files for 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 (dependant 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. 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 who information is stored about (upon written request):
- through subpoena (court ordered request for documents): and
- at the request of the statutory funding body (in each state and/or territory).

If a service user wishes to have access to information that CREATE holds about them, they need to formally advise CREATE in writing of their request. If the service user makes their request in any other way, CREATE must inform the service user that their request is 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 as to why access is being denied in writing within 14 days of receipt of the request. This should be done after consultation 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 is unable to be met, the CEO should be notified, and the person making the request will be informed and a new date negotiated.

Release guidelines – children and young people:
A child or young person of any age may ask to see information about them that CREATE holds.

File release for children and young people is governed by the following guidelines:

1. If any internal or inward correspondence (for example letters and other written material from a third party about the child or young person) on file contains the personal information of another individual, that personal information cannot be released without first deleting the personal information that relates or identifies that other individual. If the information in question cannot be deleted or blanked out, the correspondence should not be released;
2. The following can be released: case notes, outward correspondence to the individual and personal reports and documentation, for example certificates of attendance;
3. CREATE upon receipt of a written or verbal request will:
    a. review the file;
    b. photocopy all case notes and correspondence for the individual (where they do not disclose the personal information of another person);
    c. delete all references to:
        i. other children in care;
        ii. remarks that may identify a notifier (someone who has reported a concern about the child or young person); or
        iii. to any other person at all where that disclosure would have an unreasonable impact on the privacy of that other person.
4. Contact the person requesting the file to tell them to collect the file or to come in to the office to view the file; and
5. Sign a receipt of acknowledgment for the file.

Release guidelines – other agency or stakeholder:
These release guidelines are to be followed in cases where a stakeholder may request to see the information that CREATE has on file about them. Only information about the organisation or stakeholder is to be released, as outlined below:

1. The request for information release needs to be in writing and must identify the specific information requested and the reason;
2. No information is to be provided about children and young people where providing such information would have an unreasonable impact on their privacy (given the nature of CREATE's services, it is likely that this would be the case most, if not all, of the time);
3. The validity of the request should be determined by the Operations Manager. The Operations Manager should seek approval from the statutory body in the state the request derives from if deemed necessary; and

4. Before releasing information the Operations Manager should seek approval from the CEO.

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 it needs to be corrected, or the individual requests that their information be corrected. If information that has been corrected has been given to another company, the organisation is also generally 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 as to why they refuse 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.