POLICY NAME	Privacy & Information Security		
POLICY NUMBER	HR13	VERSION	1
INITIAL DATE	September 2020	REVIEWED DATE	September 2021
POLICY STATUS	☒ Active ☐ Under review ☐ Under Development ☐ Obsolete		
APPROVED BY	CEO		

PURPOSE OF THE POLICY

William Campbell Foundation (WCF) is committed to maintaining the privacy and security of information it holds in relation to all individuals including children, young people, employees, carers, volunteers, students and families.

This policy ensures that WCF handles all information in accordance with Australian Privacy Laws and other relevant legislation including how WCF collects, uses, stores, discloses and protects information about individuals and families.

This policy sets out:

- What information WCF can collect and how it is collected
- How WCF stores and protects this information
- How WCF can use and disclose this information
- What actions WCF will take if it suspects any individuals' privacy has been breached

LEGISLATION / REGULATIONS / STANDARDS

Privacy Act 1988

Australian Privacy Principals

Children and Young Persons (Care and Protection) Act 1998

Child Safe Standards

Work Health and Safety Act 2011

Data Breach Notification Scheme

POLICY STATEMENT

This policy applies to all individuals whose personal information is handled by WCF, and instructs all employees and volunteers at WCF on the handling of personal information including collection, storage, use, disclosure, access to and disposal of any information held by WCF.

Collection of information

Throughout the course of its work in maintaining the safety and wellbeing of children and young people in out of home care and seeking permanent positive care outcomes, WCF collects a range of necessary information regarding employees, carers, children and young people and birth families. The type of information collected includes personal and sensitive information, as well as relevant health information.

For the purpose of providing statutory out-of-home care and providing family support services, WCF will collect all relevant personal information including, but not limited to:

- Basic personal information – including name, address, contact numbers, financial information where applicable, photographs and other.

- Sensitive information – such as racial and cultural information, criminal histories and other.
- Health information – including health declarations, relevant medical certificates and reports, certificates of capacity, physical and psychological health information and other.

WCF collects information about individuals by the following means, only where it is relevant to the purpose of the agency and services it provides:

- Directly from the individual, whether that individual is a child or young person, carer, employee, volunteer, or applicant carer, employee or volunteer;
- From an individuals' legal guardian, family or significant others;
- From the Department of Communities and Justice (DCJ) and/or other designated Non-Government Organisations (NGOs);
- From other organisations involved in providing care and support for the respective individual (such as schools, health care providers, clinical specialists);
- From third parties as nominated by the individual, for the purpose of conducting reference checks for potential carers, staff and volunteers;
- From the individuals medical providers or health services for Work, Health & Safety and Workers Compensation purposes.

Pseudonymity and Anonymity

Under WCF's legal obligations, obligations set out in service and funding agreements, as well as the nature of work WCF performs in caring for children as a NGO, WCF is generally unable to allow any individuals to remain anonymous or act under a pseudonym.

WCF is required to have accurate identification information to:

- Assess candidates for employment, employees, volunteers, carers and other relevant people to perform probity checks and ensure their suitability for the work performed on behalf of WCF.
- Evaluate and provide the most appropriate care and support to children, young people, individuals and families.

Consent & Notification

Any individual about whom WCF collects information will be made aware of WCF's privacy policy, and consent will be sought from that individual prior to collection of that information. Where that individual is unable to give consent, consent will be sought from a legal guardian or other responsible person.

Notification will also be given to the individual about the following:

- What types of information will be collected about them
- How the information will be collected (including any third parties)
- The reason that this information will be collected
- The consequences if consent is not given to collect information
- How to access, update and seek correction of information
- How feedback or complaints can be made about a breach of privacy

Use & Disclosure

WCF only collects information relevant to its key function of ensuring the safety and wellbeing for the children and young people supported by, or under WCF's care. This information is collected under the agency's obligations as a designated agency, as well as to comply with the *Children and Young Persons (Care and Protection) Act 1998, The Children's Guardian Act 2019* and the *Child Safe Standards*. All information collected and held by the agency is done so lawfully, and is also subject to the *Commonwealth Privacy Act 1988* and the *Australian Privacy Principals*.

All information collected by WCF is kept highly confidential, and will only be shared within the agency on a need-to-know basis. Authorisation to access information will only be granted to the relevant parties, where the information is required to perform the functions of their duties, and cannot be done to the best of their ability without this

information.

Legal Requirements for Use & Disclosure

WCF may be required to disclose any information collected and held to governing bodies at any time under the following obligations:

- ***Children and Young Persons (Care and Protection) Act 1998 (NSW)***
  - *Mandatory Reporting* – where WCF or a person representing WCF suspects that a child or young person is at risk of significant harm they are required to report this to the Child Protection Helpline (a division of DCJ). Where this occurs, WCF staff are required to comply with the WCF **Allegations Policy.**
  - *Exchange of information under Chapter 16A* – WCF is required to provide information to other government or non-government agencies if requested, where the information will assist with ensuring the safety, welfare or wellbeing of a child or young person
  - *Carer Register* – WCF is required to provide specific information about carer applicants, carers, and their household members onto the NSW Carer Register
  - *Other Designated Agency checks* – WCF is required to provide information to other designated agencies that are assessing the suitability of any applicant carer/s that have any prior applications or authorisations with WCF
  - *Parent's right to information under Chapter 163* – WCF is required to disclose information about the progress and development of a child or young person in out of home care. Where this is required, WCF staff are required to follow the **WCF Disclosure of Placement Policy**.
- ***Children's Guardian Act 2019***
  - *Reportable Conduct allegations and/or convictions* – WCF is required to notify the Office of the Children's Guardian (OCG) of any allegations against employees, carers, adult household members, volunteers, students or contractors regarding reportable conduct or reportable convictions
- ***Crimes Act 1900 (NSW)***
  - *Criminal Offences* – WCF may be required to notify the police of information of a criminal offence of any employee, carer, household member, volunteer, student, contractor, child or young person, family member or other person associated with the agency.
- ***Subpoenas & Search Warrants*** – WCF may be issued with subpoenas or search warrants, where compliance is required by law. Where this occurs WCF staff are required to comply with the WCF **Subpoena Processing Policy**.
- ***Department of Communities and Justice*** – As a designated agency responsible for case management of children and young people under Parental Responsibility of the Minister (PRM), WCF is required to disclose information about children, young people, families, carers and significant others to the Department of Communities and Justice (DCJ).
- ***Office of the Children's Guardian*** – As a designated agency, WCF may be required to share records with the Office of the Children's Guardian (OCG) for auditing and accreditation purposes. Records disclosed to the OCG include:
  - Recruitment files including the personal information of all applicants for employment at WCF
  - Employee personnel files
  - Reportable Conduct Investigation Files
  - Volunteer and student personnel files, including files for all board members
  - Children and young people case management records
  - Carer records
  - Birth family records
- ***Workers Compensation*** – WCF is required to share personal and sensitive (including health) information about an employee when making a Workers Compensation claim.

Use & Disclosure Outside of Australia

WCF will not disclose any information about an individual to a third party outside of Australia unless:

- The individual concerned consents to this disclosure, or
- The disclosure is required or authorised by Australian law, or
- The recipient outside of Australia is contractually bound to comply with the Australian Privacy Principals or subject to similar laws

When disclosing information outside of Australia WCF will ensure that a secure method of transferring the information is used. Any cross-border disclosure of personal information must be approved by the CEO.

Some cloud-based electronic information storage systems used by WCF may be hosted outside of Australia. Prior to utilising a new cloud-based system, WCF will ensure that:

- There is a binding contract or agreement between WCF and the service provider which stated that the overseas host handles personal information for a limited purpose and in line with the Australian Privacy Principals
- The agreement requires any subcontractors to agree to the same obligations.
- The agreement gives WCF control of how the personal information is handled by the overseas recipient

Direct Marketing

WCF may use an individual's personal information such as name and contact details, to directly market WCF's programs and services. Direct marketing may include sending individuals communications via SMS messages, emails, letters or electronic newsletters, or requests for feedback on these programs and services.

WCF will only use personal contact information for direct marketing purposes where the individual has consented to receiving this information.

Any individual that provides consent to receive these communications can withdraw their consent at any time, either verbally, in writing, or by unsubscribing from any electronic messages or publications.

WCF marketing and communications will not include the images, photographs or other identifying information of any children or young people in care, or individuals and families that WCF provides services to.

An individual that has received services and support from WCF in the past may nominate to provide testimonials and/or images for WCF to use in their marketing materials, however the individual must provide written consent, and be over the age of 18 years. WCF will not include any information in these testimonials that breach the privacy of other individuals, This will only occur where the individual approaches WCF, and WCF will not request or approach any individuals for this information.

Storage and Security of Information

WCF takes all reasonable steps to ensure the security of personal information held by the agency, and protect it from misuse, interference, loss, and unauthorized access, destruction, use, modification and disclosure. Personal information is held by WCF and stored in both hardcopy and electronic formats.

Any records of personal information must not be destroyed or de-identified, except in cases where:

- WCF no longer requires the information for any purpose
- The information is not contained in a Commonwealth Record
- WCF is not required by law or a court tribunal order to retain the information.

Where a file must not be destroyed or de-identified, but is no longer required by WCF, the correct procedures must be followed, as given in associated WCF policies as listed at the end of this policy.

Quality of Information

All WCF employees that collect and record personal information about individuals are required to ensure that the information being recorded is accurate, current, complete and relevant. WCF employees are also required to regularly review this information to ensure that the information recorded remains current, and update this information accordingly.

Where an individual believes that the personal information held about them is inaccurate, out of date, incomplete, irrelevant or misleading, WCF will take reasonable steps to correct the information where it is appropriate and lawful to do so.

If WCF is unable to modify the record of information, or where it disagrees that the record requires correction, staff must document the request, specifying what information the individual alleges is inaccurate, incomplete, out of date, irrelevant or misleading, and the reasons why.

Access to Information

Where WCF holds personal information about an individual, that individual has the right to request access to their information. This right includes the right of a parent or legal guardian to access personal information pertaining to a child or young person under the age of 18 years.

Any request for access to information held by WCF must be made in writing where possible, and accompanied by appropriate identification.

WCF is obligated to balance an individual's right to access their personal information against the agency's legislative obligations to protect the information in a client's file.

In some circumstances, WCF may deny an individual's access to information. This includes, but is not limited to:

- Where a request is frivolous or vexatious
- Where inappropriate or insufficient identification is provided with a request for access
- Where the request may be detrimental to the individual's health, or put another person at risk of harm
- If there is a serious threat to the life or health of any individual
- Where it impacts on the privacy of others
- Where the information relates to an existing or anticipated legal proceeding involving WCF
- Where it is unlawful or would be likely to prejudice an investigation of possible unlawful activity
- Where law enforcement body performing a security function directs WCF not to provide access
- Where granting access to information would reveal information about a commercially sensitive decision making process

WCF may also refuse access under Section *7B – Organisation acting under State contract* of the *Privacy Act 1988*.

Complaints

Individuals can make a complaint when they are dissatisfied or concerned about the way their personal information has been handled, or if they believe there has been a breach of the Australian Privacy Act or Australian Privacy Principals. All complaints will be managed according to WCF's **Complaints Management Policy**, which is available on WCF's website, or on request.

Privacy Breaches

A breach of private information, also known as a data breach, occurs when any personal information recorded and held by an organisation is lost, misused, accessed by or disclosed to an unauthorised person or entity.

WCF will take all reports of suspected breaches of private information seriously, and manage these in accordance with this policy, the procedures set out below, and its legal obligations under the *Commonwealth Privacy Act 1988*.

Any breach that is deliberate or intentional are considered serious misconduct, and will result in disciplinary measures taken against the responsible staff member, including instant termination of employment.

Where any staff member mistakenly or unknowingly handles information in a way that breaches the privacy of any individuals, they could be subject to disciplinary action also, up to and including termination of employment, in line with WCF's **Serious Misconduct Policy.**

Any carers, volunteers, students or contractors found to have breached privacy of information held by WCF will also face deauthorisation or disciplinary action, relevant to their position with the agency and in accordance with their breach of Privacy and Confidentiality Agreement.

Responding to Data Breaches

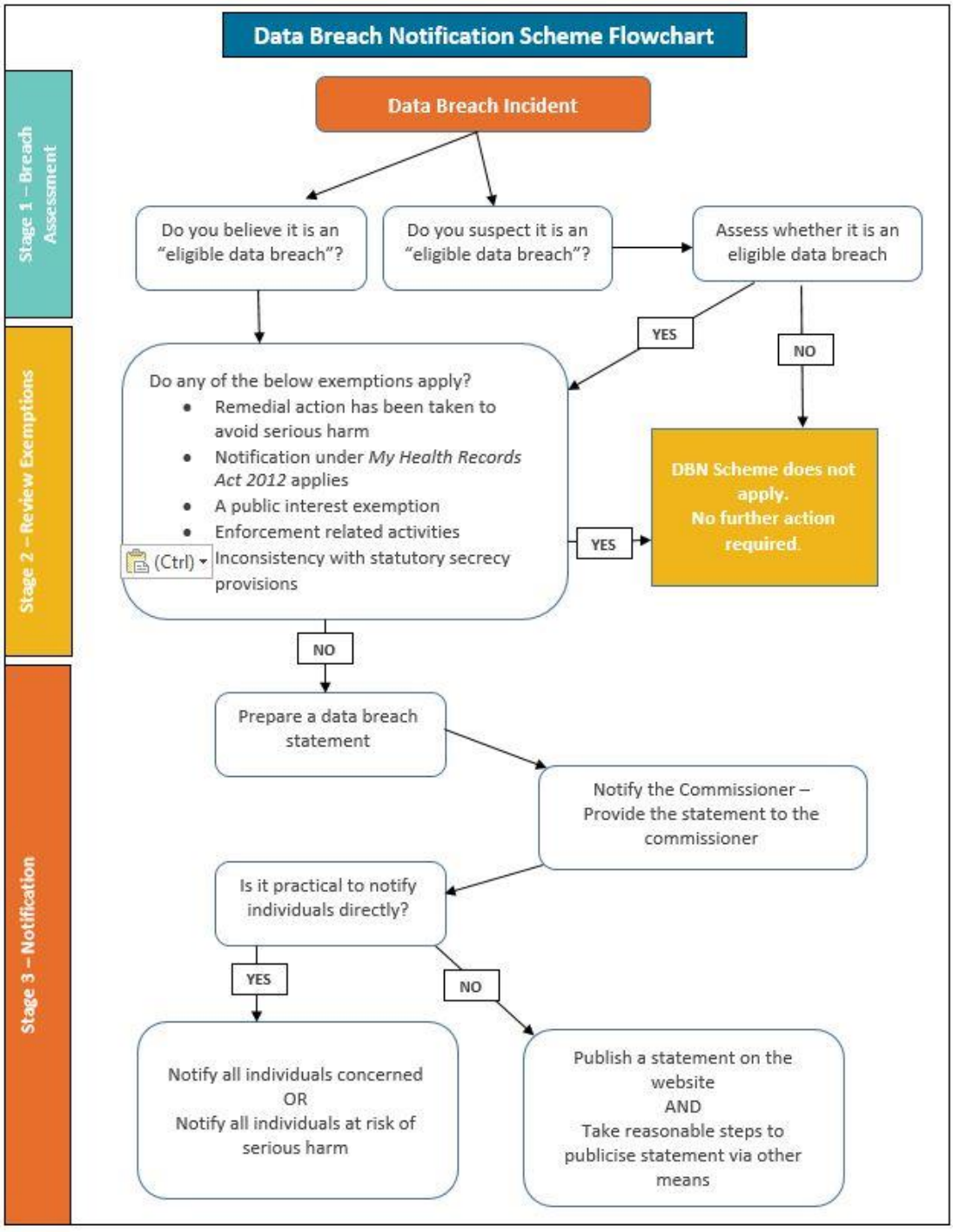
Where a staff member knows or suspects that a data breach has occurred, they are required to notify their manager or supervisor immediately, and follow the procedures listed below.

Where a data breach involving personal and/or sensitive information is considered as '*likely to result in serious harm to any individual affected*', it is considered as a **Notifiable Data Breach** under the *Commonwealth Privacy Act 1988.* Examples of serious harm may include physical, psychological, emotional, economic or financial, or reputational harm.

Where a 'Notifiable Data Breach' occurs, WCF is required by law to inform any individual/s affected of

- the circumstances surrounding the breach
- The nature of the information involved in the breach
- The steps that will be taken by WCF in response to the breach
- Any recommendations of measures that the affected individual/s should take

In response to a 'Notifiable Data Breach', WCF is also required to notify the Office of the Australian Information Commissioner (OAIC) of the details of the breach.



PROCEDURE FOR GENERAL HANDLING OF PRIVATE INFORMATION

No.	Procedure	Accountable	Due
1	All staff, students, volunteers, board members, carers and contractors are required to sign and abide by WCF's **Code of Conduct** and **Privacy and Confidentiality Agreements**.	All Staff, volunteers & contractors	On initial engagement AND annually
2	Staff that are authorised to access personal information of prospective and/or current staff and volunteers are required to sign and abide by an additional **Confidentiality Agreement.**	Administration, Finance, Human Resources &	On initial engagement AND annually

	This agreement relates specifically to the personal and confidential information held in regards to WCF as an employer, and WCF's employees.	permanent FSS staff	
3	Staff that access the personal and sensitive information of children, young people, individuals and families on personal devices are casually employed by WCF and are required to sign and abide by an additional **Confidentiality Agreement (Family Support Services Staff).** This agreement relates specifically to the personal and confidential information held on personal devices, and the security of this information.	Casual FSS Staff	On initial engagement AND annually
4	All staff are issued with WCF's **Information Technology Policy** and provided further explanation of the correct use and security of this information to mitigate the risk breaches of electronically stored information. This policy is also accessible at all times via WCF's shared common.	All staff	At induction Ongoing
5	Staff are regularly reminded of privacy rights and responsibilities and encouraged to raise concerns.	All staff	Ongoing
6	All WCF offices are protected by security alarm systems, and only authorised staff are provided with security access codes. Internal access to offices is only permitted to current staff. Where a visitor is in the office, they are to be accompanied by a staff member at all times.	Relevant staff	Ongoing
7	When not in use, all files and documents containing personal, sensitive and confidential information are stored in securely locked cabinets and file rooms. Only relevant authorised staff are able to access these files.	All staff	Ongoing
8	All staff are to be mindful of the secure handling of files and documents containing personal, sensitive or confidential information, and must never leave these documents and files unattended, or where they could be accessed or viewed by unauthorised persons.	All staff	At all times
9	Hardcopy files containing personal information of individuals must not be removed from WCF worksites, with the exception of where they are being transferred between offices for case management reallocation or archiving purposes. Exceptions to this must be approved by the CEO prior to their removal.	All staff CEO	At all times As required
10	Where files are required to be transferred between offices, appropriate **File Transfer Request** procedures must be followed, as set out in WCF's **Documentation and Record Keeping Policy**.	All staff	As required

11	Where documents containing personal, sensitive or confidential information are required to be transferred between offices in hardcopy, they are required to be placed inside a sealed document envelope and marked 'private and confidential' for transport by WCF employees only.	All staff	Ongoing
12	When required to mail documents containing personal, sensitive or confidential information, staff must ensure the documents are securely enclosed and mailed by registered post.	All staff	As required
13	All staff emails must include the confidentiality notice: *"If you are not the intended recipient you must not share, disclose, copy or distribute this communication. If you believe you have received this message in error, please ensure you delete it and notify the sender."*	All staff	Ongoing
14	When accessing files or documents containing personal, sensitive or confidential information electronically, care must be taken to ensure information is not displayed or visible to unauthorised persons.	All staff	At all times
15	All staff must handle their laptops and mobile phones in accordance with WCF's **Information Technology Policy** to ensure the security of information stored on those devices.	All staff	At all times
16	Staff are assigned different levels of access to software systems and records, dependent on their position, level of responsibility and program.	HR Manager & Administrator	At induction or as required
17	Staff are required to only log into devices or accounts using their own access details and passwords, and are prohibited from using another staff members access details in all circumstances.	All staff	At all times
18	Staff information technology (IT) usage may be surveilled at any time, as per WCF's **Information Technology Policy**.	All staff	Ongoing
19	All staff will receive data security training around the safe use of information technology.	Administrator & IT Contractor	Ongoing
20	If any staff member mistakenly accesses information (either hardcopy and electronic) without authorisation, they are required to notify their supervisor immediately.	All staff	Ongoing
21	All information stored electronically on WCF's Shared Common, and individual staff's OneDrive files are regularly backed up, with backup data stored in a secure location offsite. Staff should not save any files to their computer desk tops, as these files will not be backed up.	IT Contractor	Ongoing

22	Appropriate hardware, antivirus software and firewalls are installed and regularly updated to mitigate risks of cyberattacks and breaches.	IT Contractor & Administrator	Ongoing
23	Documents containing personal, sensitive or confidential information are disposed of in secure bins located at all office sites for secure destruction.	All staff	Ongoing
24	When discussing any personal, sensitive or confidential information or issues, all staff are required to be mindful of the volume of their voice, move the conversation to a private setting, and ensure no unauthorised persons can hear.	All staff	Ongoing
25	Staff are not permitted to email, copy, print, or take any personal or confidential information, or any other work or documents at any time, including at the end of their engagement with the agency. All work or documents created during employment/engagement with WCF remains the intellectual property of William Campbell Foundation.	All staff	Ongoing
26	WCF and its staff will inform all children, young people, carers and applicants, and individuals of their privacy rights, either verbally or in writing, in accordance with: • **Confidentiality and Privacy Policy** (for Children and Young People) • **Assessment and Selection of Carers, Guardians and Adoptive Parents Policy** • WCF's **Family Action Plan** agreement	Relevant staff	Ongoing
27	Where an individual withholds consent, or places any restrictions on their consent, staff are required to explain how this may impact on WCF's functions, activities and/or the quality of service that can be provided. If the withholding of consent means that WCF cannot provide adequate quality of care, comply with legal requirements, or fulfil its obligations as a designated agency, the individual will be advised that their involvement with WCF cannot continue.	All staff	When relevant

PROCEDURE FOR INDIVIDUALS REQUESTING ACCESS TO INFORMATION

No.	Procedure	Accountable	Due
1	All requests by individuals and third parties for access to personal information must be made in writing to WCF, and must be accompanied by current and valid photograph identification. Where a request is made verbally, the responding staff member must direct them to make this request in writing.	All staff	When a request is received

2	Once a request has been received, WCF will review and respond to the request within 30 days.	HR Manager & PSP Regional Manager	Within 30 days from a request
3	The staff member receiving a request should refer this request to the relevant PSP Regional Manager and HR Manager.	Receiving staff member	Immediately when a request is received
4	The HR Manager, in consultation with the relevant PSP Regional Manager and PSP Team Leader, will gather copies of all information related to the requesting individual for review.	HR Manager & PSP Regional Manager	Within 48 hours of a request being made
5	In accordance with the *Commonwealth Privacy Act 1988*, requests by an individual for access to information will only be granted to the person of which that information concerns or their authorised representative (i.e. solicitor), with any private information pertaining to any other individual excluded or redacted. Where access cannot be provided without compromising the privacy of another individual, access to that information will not be provided.	HR Manager & PSP Regional Manager	Ongoing
6	Where a request for access to information has been made by an authorised representative, WCF will verify their authority and the extent of that authorisation.	HR Manager & PSP Regional Manager	Prior to responding to a request
7	WCF will grant access to information where it is a requirement under the *Commonwealth Privacy Act 1988* and the *Australian Privacy Principals.* WCF reserves the right to refuse access to information that is exempt under from the *Privacy Act 1988* and *Australian Privacy Principals*. Exemptions include: • Where there is a serious threat to the life, health or safety to any individual/s or the public • Where there would be an unreasonable impact on the privacy of other individuals • Where a request is frivolous or vexatious • Where the information relates to existing or anticipated legal proceedings involving WCF • Where giving access could compromise any negotiations between WCF and the individual • Where giving access would be unlawful, or would be likely to prejudice an investigation of possible unlawful activity • Where giving access would be likely to prejudice an enforcement-related activity of an enforcement body • Where WCF has reason to suspect that unlawful activity or serious misconduct has or is taking place, and giving access would compromise WCF's ability to take appropriate action in	HR Manager & PSP Regional Manager	Within 30 days of a request being received

	relation to the matter • Where giving access would reveal information about a commercially sensitive decision making process. Determination for approval or denial of access will be reviewed by the PSP Regional Manager in consultation with the HR Manager		
8	All information exempt under the *Commonwealth Privacy Act 1988* and *Australian Privacy Principals* will be blacked out or removed from copies of any documents held by WCF prior to allowing the requesting individual access.	HR Manager	While reviewing information
9	Once all information has been reviewed and exempted information removed, the requesting individual will be provided with access by one of the following methods: • Inspecting hardcopies at one of WCF's offices, with notes and copies of documents being allowed • Providing copies to the individual's solicitor.	HR Manager & PSP Regional Manager	Within 30 days of request
10	Where access is denied, written denial must be provided to the requesting individual, including an explanation for the denial.	HR Manager & PSP Regional Manager	Within 30 days of request

PROCEDURE FOR THIRD PARTIES REQUESTING ACCESS TO INFORMATION

No.	Procedure	Accountable	Due
1	All requests by third parties for access to personal information must be made in writing to the Principal Officer, and must be accompanied by any relevant authorisations. Where a request is made verbally, the third party representative must be directed to make this request in writing.	Principal Officer	When a request is received
2	Requests for access to personal and confidential information will only be granted where WCF is legally required to do so. (See 'Legal Requirements for Use & Disclosure' in the Policy Statement for details of these requirements.)	All staff	Ongoing
3	Where a regulatory body (i.e. the Office of the Children's Guardian or the NSW Ombudsman's Office) requests access to information held by WCF, this request must be made in writing and specify a date, time and location.	Principal Officer	As requested
4	As a requirement as a designated agency, WCF will arrange for the regulatory body to have temporary access to any relevant files, including any databases used by WCF for storage of electronic files.	Principal Officer / Human Resources Manager / Administrator	As requested
5	Where the request for information is made by a third party under a Subpoena the **Subpoena Processing Policy** must be followed.	All staff	As requested

PROCEDURE FOR DATA BREACHES

No.	Procedure	Accountable	Due
1	Where a data breach (or breach of any private information) is suspected or known to have occurred, the identifying staff member must take immediate action to correct, contain, or mitigate the breach where possible. They must inform their Supervisor and the Executive Management Team.	All staff	Immediately
2	Where a breach involves electronic records held on WCF's computer systems the staff member should immediately contact WCF's IT contractor to assist in containing the breach, and: • Isolate any causes of the data breach in the relevant system, software or database • Shut down any compromised systems, software or databases • Reset log-in details and passwords • Quarantine any compromised devices	All staff	Immediately or as soon as possible after a breach
3	Where a breach involves the loss of a device (including laptops, mobile devices and portable storage drives) or physical files or documents, staff should: • Contact WCF's IT contractor immediately to remotely disable the lost device • Take measures to locate and retrieve the device/files, including searching the area where missing, reporting thefts to police, and/or contacting any relevant authorities or businesses.	All staff	Immediately or as soon as possible after a breach
4	Where a breach involves the unauthorised disclosure of information to a third party: • By email, the staff member should recall the email from the recipient, and/or ask the recipient to not read and delete the email. • By post, the staff member should contact the recipient and ask them not to open or read any contents and arrange for the materials to be collected or returned. • By online publication, staff should deactivate the link to the publication, and/or remove the publication.	All staff	Immediately or as soon as possible after a breach
5	Where there is a *significant* breach of information relating to the people WCF supports, the Principal Officer or delegated member of the Executive Management Team must notify DCJ immediately by completing DCJ's Online Notification Form https://www.onlineforms.dcj.nsw.gov.au/ics/Pages/Cyber-Security-Incident-Form.aspx	Principal Officer / Executive Team	Immediately

	A follow up email must be sent to the DCJ Contract Manager as soon as possible and within 24 hours. Significant breaches include one or a combination of the following: • Breaches involving a malicious cyber-attack on WCF 's IT systems • Breaches of large numbers of people supported by WCF		
6	DCJ must be notified for all other breaches that relate to children, young people and their families where they are supported by WCF by phone and email. WCF will consult with DCJ's Contract manager for direction on further actions required to inform the children, young people or families affected.	Executive Team	Within 24 hours of the breach
7	The reporting staff member must then complete the WCF **Data Breach Incident Report Form** and submit the form to the Executive Team attaching any relevant evidence to the report (e.g. screenshots, emails, etc.) If necessary, the form can be completed in consultation with a member of the Executive Team if required.	Reporting staff member & Executive Team	Within 24 hours of breach
8	The Executive Team will perform a preliminary investigation to assess the severity of the breach based on the **Data Breach Incident Report** completed and using the flowchart below, evaluate whether the breach qualifies as an 'eligible data breach' under the **Data Breach Notification Scheme,** where the breach poses a serious risk of harm to any of the individuals whose personal information is involved.	Executive Team	Within 48 hours of the breach
9	Where the breach affects people supported by WCF, a the **DCJ Information Security Incident Report** must be completed detailing information and findings from the previous 2 steps. This completed form must be submitted to the DCJ Contract manager within 48 hours of the initial notification to DCJ.	Executive Team	Within 48 hours of notifying DCJ
10	Where necessary, DCJ may take further actions, and depending on the nature and severity of the data breach, actions may include temporarily restricting WCF's access to DCJ electronic systems or digital platforms. WCF's Executive Team will support the process and ensure DCJ are provided with any necessary information.	Executive Team	Where relevant
11	Where the breach is identified as an eligible data breach under the Data Breach Notification Scheme, the CEO/Principal Officer and the Board must be notified, if not already aware.	Executive Team	Within 48 hours of the breach
12	Where the breach is identified as an 'eligible data breach' under the **Data Breach Notification Scheme**, the delegated Executive Manager	Executive Team	Within 7 days

	will prepare a Data Breach Statement and notify the Commissioner (OAIC) of the breach.		
13	A statement must be prepared as soon as possible after the breach to notify all individuals whose information has been breached. Where it is not known specifically which individuals have been affected, all individuals likely to be affected should be notified. Consultation and advice should be sought from DCJ prior to making notifications to people supported WCF. This statement should be made verbally where possible, and followed up in writing, and should include: • what kind of information was involved in the breach • a description of the breach (i.e. date of the incident, date of detection, how the breach occurred and who is likely to have accessed to the information) • what measures have been taken by WCF in response • any recommendations to the individuals to protect themselves against any risks faced due to the breach. This may be general information to all affected, or specific information to particular individuals. • the contact information for a nominated staff member for any questions or follow up.	Principal Officer or delegated Executive Manager	Within 7 days

POLICIES/FORMS ASSOCIATED WITH THIS POLICY

Form Name	Pathway
HR4 Information Technology	Policies → Human Resources
HR6 Recruitment of Staff and Volunteers	Policies → Human Resources
HR16 Subpoena Policy	Policies → Human Resources
PSP7 Privacy and Confidentiality	Policies → Permanency Support Program
PSP9 Health	Policies → Permanency Support Program
PSP17 Documentation & Record Keeping	Policies → Permanency Support Program
PSP18 Disclosure of Placement	Policies → Permanency Support Program
PSP19 Assessment and Selection of Carers, Guardians and Adoptive Parents	Policies → Permanency Support Program
PSP24 Carer Register Policy	Policies → Permanency Support Program
Data Breach Incident Report	HR → Forms → Information Technology
DCJ Information Security Incident Report	HR → Forms → Information Technology
Privacy & Confidentiality Agreement	Policies → Human Resources → Code of Conduct and Privacy Agreement
Confidentiality Agreement (Admin)	HR → Forms → Confidentiality Agreements

Confidentiality Agreement (FSS)	HR → Forms → Confidentiality Agreements
Code of Conduct	Policies → Human Resources → Code of Conduct and Privacy Agreement
File Transfer Request Form	Admin → Forms → Archives
Data Breach Preparation and Response Guide (OAIC)	HR → Resources

POLICY HISTORY:

Version	Date Approved
1	September 2020
2	September 2021

DUE FOR REVIEW	September 2023