It is important that this Policy accurately reflects the current situation and organisational requirements of Conciliation Resources Australia (CRA) / the South East Asia and the Pacific (SEAP) Department. It is the responsibility of the SEAP Human Resources department to review this Policy every three years or in the event of any organisational changes or statutory changes, make any updates if necessary and receive approval by the SEAP Department Director and CR Executive Director before publishing it.

CRA and SEAP are used interchangeably throughout this document. CRA is used when referring to the legal structure based in Australia and SEAP will refer to the collective department structure.

### Table of Contents

- **Purpose and Scope** ................................................................. 3
- **Definitions** ................................................................. 3
- **What is Personal Information and why do we collect it?** ................................................................. 4
  - Sensitive Information ................................................................. 4
- **Principles** ........................................................................ 6
  - Lawful processing .................................................................... 6
  - Individual rights .................................................................. 7
  - Informed consent ................................................................... 8
  - Satisfaction of principles and compliance with the regulations ................................................................. 8
- **Applying the policy** ................................................................. 9
  - Requests for access to or deletion of personal information ................................................................. 9
  - Conciliation Resources’ IT systems ................................................................. 9
- **Information requested by an employee or former employee** ................................................................. 10
- **Providing references** ................................................................. 10
- **Contacts and Fundraising Database** ................................................................. 11
- **Shared files and group-restricted server files** ................................................................. 11
  - Website e-newsletter .................................................................. 12
  - Online donations .................................................................. 12
  - Recruitment ........................................................................ 12
  - Personnel and payroll .................................................................. 13
  - Publication mailings .................................................................. 14
- **Data security** ........................................................................ 14
  - Storing data securely ................................................................ 14
  - Transferring data internationally ................................................................. 15
Purpose and Scope

Conciliation Resources is registered as Conciliation Resources Australia in Australia with the Australian Charities and Not-for-profits Commission (ACNC) and operating as a public company limited by guarantee.

This policy outlines Conciliation Resources’ commitments to respect the privacy of people’s personal information and observe the relevant data protection legislation. It is designed to enable Conciliation Resources’ staff and others to be clear on what our data protection principles, commitments and operating practices are.

Conciliation Resources is registered with the Information Commissioner’s Office (ICO) in the UK as a data controller and holds and processes certain personal data for the purposes of carrying out its aims and objectives.

This personal data, whether it is held on paper, electronically or in other forms, is subject to the appropriate legal safeguards as specified in the UK Data Protection Act 2018 and The Privacy Act 1988. This policy complies with the requirements of the UK General Data Protection Regulation (GDPR) and comply with the Australian privacy principles.

Conciliation Resources Australia (CRA) holds and processes personal data on past, current, and prospective board members, staff, volunteers, donors, individuals and organisations we work with; and suppliers and others with whom we communicate.

CRA regards the lawful and correct treatment of personal information as crucial to our successful operations. This involves taking precautions against physical loss or damage and ensuring that access and disclosure are restricted. All staff are responsible for ensuring that:

- Personal data is only retained when necessary, and for valid reasons
- Any personal data held is kept securely
- Personal information such as mobile phone numbers, social media ‘handles’ (online names) or email addresses, are not disclosed to any unauthorised third party, without the subject’s consent.

Conciliation Resources’ International Safety and Compliance Manager is the Data Protection Officer named in our registration with the Information Commissioner’s Office (ICO). If in any doubt about any aspect of handling personal data, you should consult the International Safety and Compliance Manager (Chief Operating Officer if International Safety and Compliance Manager is not available).

We also use third-party providers and platforms in the course of our work and operations. These are detailed in the policy and in our Privacy Notice.

Definitions

Consent: According to The Australian Institute of Family Studies (AIFS) Consent is an individual's free agreement to participate in an activity. Consent can only be given if it is free and voluntary, without fear, coercion, intimidation or anything else that inhibits free agreement. It is not enough to say that an individual consented just because they did not refuse or resist. Legal definitions of consent vary between Australian state and territory jurisdictions For detailed definitions of consent, refer to https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/consent-to-the-handling-of-personal-information

---

1 Is also referred to Privacy Act in this policy.
**Employee:** A person that’s hired to provide a service to a company either on a full-time, part-time or casual basis in exchange for payment. **Other known terms:** staff and worker.

**Informed Consent:** Your consent is only valid if you’re aware of the consequences of giving or not giving your consent at the time you make the decision. An organisation or agency should:

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


**The Privacy Act 1988 (Privacy Act):** is the principal piece of Australian legislation protecting the handling of personal information about individuals. This includes the collection, use, storage and disclosure of personal information in the federal public sector and in the private sector.

**The General Data Protection Regulation (GDPR):** is a European Union regulation on information privacy in the European Union and the European Economic Area. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

**Special category of personal data:** Certain types of sensitive personal data are subject to additional protection under the GDPR. These are listed under Article 9 of the GDPR as “special categories” of personal data.

The special category of personal data is known by ‘Sensitive Information’ in Australian Privacy Act.

The ‘Special category data’ and ‘sensitive information’ are used interchangeably in this policy.

**What is Personal Information and why do we collect it?**

Personal Information is information or an opinion that identifies an individual. Examples of Personal Information we collect includes names, addresses, email addresses, phone numbers.

This Personal Information is obtained in many ways including interviews, verbal communications, correspondence, by telephone, by email, via our website www.c-r.org, from media and publications, from other publicly available sources, from cookies. We don’t guarantee website links or policy of authorised third parties.

When we collect Personal Information, we will, where appropriate and where possible, explain to you why we are collecting the information and how we plan to use it.

**Sensitive Information**

Sensitive information as per the Privacy Act is to include information or opinion about such things as an individual’s racial or ethnic origin, political opinions, membership of a political association, religious or philosophical beliefs or affiliations, membership of a trade union or other professional body, sexual orientation, criminal record, health or genetic information.
We may collect sensitive information about you:

- where you consent
- when the collection is authorised or required by law
- when the collection is otherwise allowed under the Privacy Act.

The kinds of personal information we may collect includes all of the following.

Information about you, such as your:

- full name
- postal and residential address
- gender
- date of birth
- contact details.

Information about your circumstances for, employment and recruitment, in a time of emergency and disaster, such as your:

- signatures
- employment status and history
- education status
- cultural and linguistic background
- citizenship and visa status
- passport and travel movements
- health, allergies, medical condition including covid vaccination certificate
- disabilities

Information about your family and other related persons for emergency contact, next of kin, and proof of life form, such as any:

- partners
- children
- dependants
- carers
- nominees or authorised representatives.

We also collect information about you for employment purposes and to deliver payments, including:

- superannuation details
- tax file numbers\(^2\) (CRA do not keep printed hard copy of TFN number or the TFD).
- ABN number if the employee is a Sole trader or has a company proprietorship
- [add what we collect from partners]

We may also collect information through our IT department in the UK, such as:

- pages you visit
- online forms you fill in
- searches you make.

Online activity

- Cookies
- Website analytics – to better understand the traffic on the website

\(^2\) CRA adhere to the Privacy (Tax File Number) Rule 2015 for the collection, storage, use, disclosure, security and disposal of TFN information.
Principles

These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transporting and storing personal data. Staff, volunteers or any other people or organisations associated or working with Conciliation Resources who obtain, handle, process, transport and store personal data for Conciliation Resources must adhere to these principles.

Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that, “the controller [i.e. Conciliation Resources] shall be responsible for, and be able to demonstrate, compliance with the principles.”

Lawful processing

Under article 6 of the GDPR, a lawful basis for processing must be identified and documented before personal data can be processed. The lawful bases available are:

a) Consent of the data subject [the person whose data is stored]

b) Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract

c) Processing is necessary for compliance with a legal obligation

d) Processing is necessary to protect the vital interests of the data subject or another person

e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

f) Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject
The special categories of data can only be processed if one of the following applies (Article 9(2)) of GDPR:

a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes[…];
b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection[…];
c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
e) processing relates to personal data which are manifestly made public by the data subject;
f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
g) processing is necessary for reasons of substantial public interest, […] which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care and services […] or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, […] which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)[…] which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Individual rights

Individuals have specific rights in relation to their personal data under GDPR:

a) The right to be informed
b) The right of access
c) The right to rectification
d) The right to erasure
e) The right to restrict processing
f) The right to data portability
g) The right to object
h) Rights in relation to automated decision making and profiling
Informed consent

When obtaining consent, you should ask yourself:

- Does the person know why you are collecting their data?
- Does the person know how their data will be processed?
- Does the person know who could have access to their data?
- Does the person know how long we will store it for?
- Does the person know how to withdraw consent at a later stage?

When obtaining consent from participants, you should ask yourself:

- Does the person know why you are collecting their data?
- Does the person know that they can stop providing their data at any time and nothing bad will happen? Be clear that it is their story, photo, information and they own it.
- Does the person know that they and their community will not receive anything in exchange for their data?
- Does the person know how their data will be processed?
- Does the person know who could have access to their data?
- Does the person know how long we will store it for?
- Does the person know how to withdraw consent at a later stage?

Satisfaction of principles and compliance with the regulations

CRA has in place appropriate management controls and uses strict criteria to:

- Observe fully the conditions regarding the lawful and fair collection and use of personal data
- Meet its obligations to specify the purposes for which personal data is used
- Collect and process appropriate personal data only to the extent that it is needed to fulfil operational or any legal requirements
- Ensure the quality and accuracy of personal data held to the best of Conciliation Resources’ ability
- Apply strict checks to determine the length of time personal data is held
- Ensure that the rights of individuals about whom the personal data is held can be fully exercised
- Take the appropriate technical and organisational security measures to safeguard personal data
- Ensure that personal data is not transferred outside the UK and designated ‘adequate protection’ countries, without suitable safeguards

Conciliation Resources is registered with the UK ICO as a Data Controller on its public register of data controllers (Registration number Z9847634). Conciliation Resources holds personal data for the following six purposes:

- Realising the objectives of Conciliation Resources
- Staff administration
- Advertising, marketing and public relations
- Accounts and records
- Administration of membership records
- Fundraising
Applying the policy

Any breach of this policy will be taken seriously and may result in disciplinary action, up to and including dismissal.

Every staff member, volunteer or consultant working for Conciliation Resources is expected to adhere to the policy at all times. Any staff member or volunteer who believes that the policy has not been followed in respect of their own personal data or that of others should raise the matter with their line manager or with the International Safety and Compliance Manager.

Each database or file storage system has a designated person responsible for the implementation of the Data Protection Policy in relation to that particular system. Members of staff who wish to use the data may do so only with the authority of the person responsible for the particular database or system, who will ensure compliance with this policy.

The persons responsible for each database or set of personal information is as follows:

- Contacts and Fundraising Database – CR Grants and Development Manager
- Shared files and group-restricted server files – CR Chief Operating Officer
- Website e-newsletter – CR Head of Communications
- Online donations – CR Head of Fundraising
- Recruitment – CRA Human Resource and Compliance Manager
- Personnel – CRA Human Resource and Compliance Manager
- Payroll – CRA Finance Manager

Requests for access to or deletion of personal information

Any request from a person asking to see their personal data held by CRA; have their details amended; be removed from a mailing list or database; or any other related enquiry, should be sent to the SEAP Operations Director. It is helpful if such requests and enquiries are also copied to the relevant person named above, to facilitate swift processing.

Any enquiries will be responded to in accordance with The Privacy Act 1988 and with GDPR. Compliance with requests for data to be erased may be restricted by CRA’s duties under other legislation, such as requirements to keep financial or employment records for tax purposes.

CRA and will ensure that a response is provided within 30 days of receipt of a request. Subject access requests are processed in accordance with our Subject Access Request Policy.

If a data subject asks CRA to delete their personal data, we will process the request in line with our Deletion Policy.

Conciliation Resources’ IT systems

- When using any of these systems for the storing of personal data, it is the individual staff member’s responsibility (if necessary, in consultation with the person with overall responsibility for the system or the Chief Operating Officer) to ensure that they undertake the following:
  - Determine and document a legal basis for storing/processing the personal data
  - Provide any privacy notices required to the data subjects whose personal data is being processed
  - Ensure the necessary security measures are taken (e.g., password-protecting files)
  - Keep the personal data up to date and accurate
• Review the data, assign a new legal basis if necessary and delete when no longer needed

For more information on the above, see the GDPR training presentation or Data Protection Toolkit.

Information requested by an employee or former employee

If an employee or former employee requests access to their own employment records, you must make a legible copy available for them to inspect and copy. If the employee record is kept at the workplace, you must make the copy available there within 3 business days or post a copy to the employee within 14 days after receiving the request. If the employee record is not kept at the workplace, you must make a copy available or post it to the employee as soon as practicable.

Providing references

You may be approached to provide employment references about former or current employees. You won’t breach privacy laws if you provide personal information that relates directly to the employee’s employment, but you can still ask for their consent. This can usually be assumed if they have already asked you to be a referee. If they haven’t, you should consider seeking their consent before disclosing information about them.

Consider what information is appropriate to provide in a reference. Keep your comments focused on the employment relationship to avoid any possible privacy issues. This includes the employee’s skills, performance, conduct, their type of employment and length of employment. It is generally not appropriate to disclose private information about a current or former employee (for example, their medical history). As mentioned, Commonwealth privacy laws set a higher standard for collecting and handling sensitive personal information.

What information is not considered private, confidential and sensitive:

• electronic communications and social media aren’t private
• the business can delete data and information employees have put into its systems at any time
• what is and isn’t acceptable use for email, social media and internet at work
• not to disclose personal information about customers or colleagues (including images of them) through social media, email or other mediums
• the business monitors compliance with its privacy, social media and acceptable usage policies, and the possible consequences of breaching these policies
• what information is recorded and kept by the business (such as content and patterns of employees’ emails and browsing activities, or location information) and who can access these records
• what, if any, areas are under surveillance (including CCTV and drones) and who has access to the information (State and Territory laws may limit when surveillance can be conducted in the workplace and elsewhere. See Links and resources for links to information in your State or Territory).
• employee attendance at work (for example, to satisfy workplace health and safety requirements).
Contacts and Fundraising Database

For its own activities CRA maintains a database of contact information about individuals and organisations who we work with. This is password-protected and only accessible to CRA staff, including volunteers and consultants where this is necessary.

- The information on this database may include a person’s name, address, email address, telephone/fax number(s), job title and employer, work-related interests, plus details of their involvement with CRA including funding given, events attended and the relationship of the individual to CRA (e.g. a mediator in a conflict or programme partner).
- Professional and other contacts are added to this database, using information from a business card or other exchange of contact details, that CRA staff have received during business contact with the individual.
- The legal basis for processing the personal data on this database is legitimate interest for professional or business contacts and consent for fundraising contacts.
- Contacts deemed to be kept on legitimate interest grounds will be reviewed at least every three years without recorded contact. See the Legal Basis Guide for more information.
- Staff must not add or keep personal data that may be defamatory, inappropriate or unnecessary for the purposes for which the data is kept.
- Staff must not add to the Contacts Database sensitive personal data (‘special category data’ – see above) other than with the explicit consent of the data subject to process the data for a specific purpose; for example, to arrange focus groups of LGBTQ+ people or a particular religious group.
- Individuals may directly ask for their data to be removed from any of CRA’s databases. Where data is kept with the consent of the data subject, CRA will seek to renew this consent after four years without any recorded contact. Data will be removed if consent is sought and not given.
- All individual contacts will have a staff member or team assigned to them, and those staff are responsible for ensuring that the personal data and other information for that contact is kept up to date.
- Data will be removed when they are believed to be out of date or no longer necessary for the work of CRA.

Shared files and group-restricted server files

Conciliation Resources maintains a system of ‘Shared files’ on its server where various documents are stored for each team in the course of their work. This may include documents that contain personal data. Only staff with a system’s login, and contracted IT staff, are able to access these folders and files.

- Documents on Shared files containing personal data are likely to take the form of lists of activity participants and event invitees, lists of approved suppliers and donor 1 https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-forprocessing/special-category-data/ reporting documents, however other types of documents may also be stored.
- Staff must only keep documents containing personal data on Shared files for as long as is necessary for the duration of a project, fulfilment of a legal /contractual obligation or another purpose.
- Any documents stored on shared files that contain personal data should be password protected.
- The storing of personal data on documents on Shared files is likely to come under legitimate interest as a legal basis but this will need to be assessed and documented on a case-by-case basis.
• Explicit and documented consent is required from the data subject to store any ‘special category’ data.
• Where sharing data stored on shared files or Google drive by email, where possible CR personnel must send a Google drive link or a shared files filepath, rather than emailing the data as an attachment.

Website e-newsletter
Conciliation Resources sends mass emails about its news and latest work via a third-party e-newsletter system.
• Users indicate their preferences to receive these emails by actively subscribing via the Conciliation Resources website, giving their consent for data to be processed. A privacy notice with a link to Conciliation Resources’ full Privacy Policy is supplied to users at the time of subscription and is available to them at all times.
• Users subscribe via a double opt-in process.
• Users’ preferences are stored in the database 3. All recipients are given the opportunity to opt-out of these communications at any time via an ‘unsubscribe’ link contained in every e-newsletter.
• Individuals may ask Conciliation Resources directly for their details to be removed from the Mailchimp database or use the unsubscribe link in any e-newsletter to withdraw their consent.

Online donations
Donations which Conciliation Resources receives online are processed by a third-party provider.
• CAF collects the personal details of donors (name, contact details and payment details) and then processes the donations on Conciliation Resources’ behalf.
• The provider stores all donor details and provides us with the names, contact details and donation amounts of individuals who make online donations via a secure online platform. They do not share payment details with Conciliation Resources.
• Conciliation Resources does not store any of these donor details directly on our internal systems.
• The provider has a legal obligation to HM Revenue and Customs to keep donor details with GiftAid records for a minimum period of six years from the end of the accounting period they relate to.

As an EU-based organisation, the provider is subject to EU data protection regulations. For more details of how the provider manages personal information visit: https://www.cafonline.org/navigation/footer/privacy

Recruitment
CRA gathers personal data for the purpose of staff recruitment. Data obtained through recruitment are not used for any other purpose. This data is processed as detailed below:
• Only relevant personal information is gathered through the application form, and candidates are informed that the personal information obtained through the form will be used according to this policy.
• Applicants are informed if any of the data they supply is to be checked with a third party.
• Information is kept securely and not disclosed to a third party except those involved in that particular recruitment process.
• Staff involved in recruitment are aware of data protection regulations and are required to handle personal information with sensitivity and in accordance with the regulations.
• Identifiable personal data of applicants who are not shortlisted is not available to staff members outside the Human Resources department.
• Application forms of unsuccessful short-listed candidates, all score sheets and interview notes must be passed on to the Human Resources Manager who will keep them securely for a period of twelve months from the position being filled and then destroy them.
• Electronic versions of application forms of unsuccessful short-listed candidates are also deleted after twelve months of the position being filled.
• Diversity monitoring is conducted through an anonymous webform so that it is not associated with identifying information relating it to an individual person.

Personnel and payroll

Personal information about staff, consultants, volunteers and board members is processed primarily for statutory Human Resources purposes. Staff data is kept securely on a third-party cloud-based platform.

• Such information includes (where applicable) contact details, next of kin details, bank account details for salary payment, time taken off for sickness, leave and similar details.
• Accident information is kept in an incident log maintained by the SEAP Operations Director.
• All personal information whether maintained electronically or on paper is only accessible to the Human Resources team and the payroll and finance team, the individual’s direct line manager and any other staff as identified in other policies and procedures, where it is necessary in order for CRA to carry out its duties as an employer. This information is available to third parties only where necessary for CRA to carry out its duties (e.g. HR system provider, insurance company and bank for salary payments).
• Work-based contact details (work telephone numbers and email address) for staff, consultants, volunteers and board members, are available to other staff, consultants, volunteers and board members to enable them to carry out their work. This data is available through the Conciliation Resources intranet, internal email directories and internal telephone directories.
• At the point that a staff member, consultant or volunteer leaves CRA, they may choose to give consent to their personal contact information being added to the contacts database (such as Podio). Consent must be recorded as detailed above (see ‘Contacts and Fundraising Database’).
• Basic contact information (i.e. address) is required until at least the end of the financial year in order to send P60s or other pay or tax details/summary to former staff.
• Sensitive personal data (‘special category data’), is collected with explicit consent, and used only for essential purposes such as for travel, incident response and insurance purposes.
• All other personnel records are managed in accordance with Conciliation Resources’ Retention of Records Policy.
• Staff leaving Conciliation Resources are subject to the confidentiality clause in their employment contract whereby they are prohibited from disclosing any confidential information to which they may have had access during their employment at Conciliation Resources.

For more information about the security measures taken by the HR system provider, visit: https://help.employmenthero.com/hc/en-au/articles/5839177043983-Privacy-Policy
Publication mailings

Conciliation Resources sends occasional publication postal mailings to selected professional contacts.

- The contact details of recipients of Conciliation Resources’ printed publications are stored in the contacts database of professional contacts. Recipients are identified from the database: people who have requested printed publications, and people whose professional interests indicate a strong likely interest in the subject of the publication.
- For purposes of distribution of printed publications, postal addresses of recipients are shared with a mail house under a strict written agreement which prevents sharing and requires the secure storage of personal data only for the time necessary to complete the task.
- Only the designated staff member coordinating a mailing of a specific, printed publication is authorised to share the postal addresses of recipients with the company that handles the distribution of Conciliation Resources’ publications.

Data security

All CRA staff, consultants and volunteers must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the Chief Operating Officer will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

Personal data must not be shared with any unauthorised individual or organisation outside of CRA without the explicit consent of the data subject or another documented legal basis.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it.
- Printed data should be shredded when it is no longer needed.
- Data stored on a computer should be protected by strong passwords and, where possible, two-factor authentication. We encourage all staff to use a password manager to create and store their passwords.
- All CRA computers must lock their screens when left idle for five minutes, requiring a password to unlock. We encourage all staff to lock their screens when they are going to be away from their desks regardless of the duration.
- For each Conciliation Resources’ IT system, each user must have a separate account with a distinct password so that users’ access can be permitted or restricted on an individual basis as appropriate for their work.
- CRA’s laptop/portalable computers, mobile phones and tablets must be encrypted.
- CRA’s laptop computers are encrypted with a centrally-managed key to allow for data recovery. This must be applied by the IT department during the setup of a new laptop computer.
- Android and iOS devices are automatically encrypted when a lock is enabled: locks must be secure pin codes, patterns or passwords and must activate within five minutes of ‘idle’ time.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used. Discs or memory sticks that hold personal data or other confidential data must be encrypted.
- If a staff member, consultant or volunteer uses equipment that does not belong to CRA to carry out work for CRA, they must ensure that it meets the same security requirements as CRA’s equipment.
  i. Laptops must be encrypted and appropriate recovery arrangements should be put in place, equivalent to CRA’s key.
ii. Each user of the computer or device must have a separate account with a distinct password, so that other users of the computer cannot access CRA’s data.

- The Chief Operating Officer must approve any cloud or other external system used to store data.
- Servers containing personal data must be kept in a secure location, away from general office space. Conciliation Resources’ onsite servers are kept in a secure room, locked with a key and a coded lock.
- All servers containing sensitive data must be approved and protected by security software and a strong firewall.

If staff are unsure about any aspect of data security, they should seek the guidance of the IT Team or Chief Operating Officer.

Transferring data internationally

There are restrictions on international transfers of personal data. Personal data must not be transferred across borders without first consulting the International Safety and Compliance Manager.

Any third-party providers we share data with who are based outside the UK and Australia that are not approved ‘adequate protection’ countries, are carefully selected to ensure they have adequate safeguards in place.

We undertake a range of due diligence before, during and after engagement with international partners, in order to ensure that personal data is kept in line with our standards.

Access to data

Staff, volunteers and other subjects of personal data held by CRA have the right to access any personal data that is being kept about them. Data subjects also have the right to request correction of their data, opt-out of certain processing of their data and to have their data deleted. Except when any of these rights are superseded by legal or contractual obligations. See the above section on ‘Principles’.

Any person who wishes to exercise one of these rights should contact the International Safety and Compliance Manager. The request for access to their data should be made in writing. CRA’s reserves the right to charge a ‘reasonable fee’ when a request is manifestly unfounded or excessive, particularly if it is repetitive. CRA may also charge a fee to comply with requests for further copies of the same information. If personal details are inaccurate, they will be amended upon receipt of a written request detailing the inaccuracies along with the correct information. All requests will be responded to within one month of receipt.

The computer systems and all information held on them remain CRA’s property at all times. With express authorisation from the email account holder or from the Chief Operating Officer (or in their absence, another member of the Executive Management Team), the IT Manager or another authorised member of staff may access the files, telephone messages or email account of another user. Computer hard drives and online or server accounts may also be accessed by IT staff for maintenance, security and administration purposes. See IT Policy.

Retention of data

CRA will keep some forms of information for longer than others. As part of our Risk Management Strategy, Conciliation Resources carries out regular backups of data held on its internal databases and of all files held on its servers. The backups are either done externally or on our servers on a regular basis and at any point in time, data that is up to two years old can be retrieved. Only the Chief Operating Officer and designated IT staff have access to the
old data. In the event that data is restored from the backup, the staff member carrying out the procedure must be sensitive to the data protection implications of this action.

In the event of a request from a data subject for Conciliation Resources to delete their personal data, the Deletion Policy should be followed.

Privacy notices

In order to fulfil the right of individuals to transparency and to fulfil our obligations under data protection legislation, we provide privacy notices to data subjects whose personal data we process. As well as a full Privacy Notice which is available on our website, we provide separate privacy notices in different formats to data subjects at the point of collecting their data, including when people sign-up to receive our e-newsletters.

We also provide privacy statements to staff, consultants and volunteers. See the Data Protection Toolkit for more information. In addition, we include the following privacy information:

Email sent from a Conciliation Resources’ email address (footer):

This email is intended only for the named addressee(s) and may contain confidential and/or privileged material. If you have received this email in error, please notify Conciliation Resources immediately using seapdepartment@c-r.org and delete the message.

E-newsletters:
You are receiving this email because you subscribed via the Conciliation Resources website (www.c-r.org) to receive such mailings.

The above statement appears next to an ‘unsubscribe from this list’ option and an ‘update subscription preferences’ option, where users can decide on which types of mailings they want to receive, e.g. region-specific or job opportunities.

Training

All staff, volunteers and board members receive training on our Data Protection Policy and related policies. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policies and procedures.

Training is provided through a compulsory in-house seminar, as well as documented guidelines and ad-hoc support. This training and guidance covers:

- The law relating to data protection
- Our data protection and related policies and procedures

All the information related to Data Protection are uploaded on hub.

Contact

If you have any queries about this or related policies, please contact our Data Protection Officer, the SEAP Operations Director.
Related Policies

- Data Retention Policy
- Data Breach Policy
- Erasure Request Policy
- Objection to processing Policy
- Rectification Requests Policy
- Subject Access Request Policy
- IT Policy
- CRA Anti-Fraud, Bribery and Corruption Policy
- Complaints Policy