



DATA PROTECTION AND DIGITAL SECURITY POLICY

MIGRANT WORKERS CENTRE

Approved by the Board of the Migrant Workers Centre Ltd on 29 April 2025

1. BACKGROUND

At the Migrant Workers Centre Ltd (MWC), we organise, support, represent and advocate on behalf of migrant workers.

The MWC is committed to ensure the privacy and confidentiality of all data we collect and record from workers, to uphold the safety and security of our digital data management, and to comply with our obligations in managing any digital security risks.

The MWC recognises the sensitive nature of the data we collect and seek to always protect the workers we are collecting the data from.

We protect our data in several ways, including by adhering to the Digital Security Protocols set out in this document.

Data protection is everyone's responsibility. Staff are to be trained on digital security protocols.

The MWC is bound by the *Information Privacy and Data Protection Act 2014* (Vic) and the *Health Records Act 2001* (Vic).

As a community legal service, we also have obligations to clients of our legal service in relation to the confidentiality of their information.

The main regulatory references for this Policy are the:

- *Information Privacy and Data Protection Act 2014* (Vic)
- *Health Records Act 2001* (Vic)
- Minimum Cybersecurity Expectations of the Victorian Legal Service Board + Commissioner (VLSBC).

2. SCOPE

This Policy applies to the MWC's directors, employees, secondees, contractors, students and volunteers (collectively, "staff") in managing, maintaining, and upholding data protection and digital security pertaining to work carried out for or on behalf of the MWC.

This Policy is to be read in conjunction with the MWC's Privacy Policy. Our privacy policy is available on our website or on request and is attached to this document as *Appendix 1*. What personal data we collect and how we collect, use and disclose personal data is set out in our privacy policy.

Data Protection refers to the confidentiality and integrity of all digitally stored information held by the MWC, including any personal and sensitive information about the MWC's:

- staff (or prospective staff)
- clients, potential clients and service users, and
- people who provide donations or goods and services to the MWC.

Digital Security refers to the measures that we undertake to:

- uphold Data Protection
- mitigate or avoid any risks and threats that may compromise Data Protection
- minimise any consequences from any compromise to Data Protection.

3. DATA PROTECTION & DIGITAL SECURITY

How we store data

At the MWC, we store data in several ways, including, but not limited to:

- Online database systems and digital platforms, including but not limited to ActionStep, MailChimp, NationBuilder, Slack and Megaphone
- In digital files stored on SharePoint or work devices such as computers or laptops
- In removeable media like USB sticks, memory cards, and external hard disks
- In some circumstances, on paper until transferred into electronic form.

Who can access data

The people who can currently access our data are permanent employees and external IT contractors who help us manage our data systems.

The MWC is a small organisation with less than 15 permanent employees. However, as our operations grow, we may engage the support of volunteers, secondees, labour hire, contractors, service providers, or students through student placements. Some of them may be able to access data held by the MWC.

We do not sell data under any circumstances.

4. DIGITAL SECURITY PROTOCOLS

MWC staff may hold accounts across its digital platforms, including but not limited to: email, SharePoint, ActionStep, Slack, MailChimp, NationBuilder, and Megaphone.

These protocols must be adhered to across all digital platforms and when dealing with all MWC data.

A. Password management for MWC accounts

1. Passwords should be generated, auto-filled, encrypted, and securely stored using a password management software.
2. All staff are obliged to use a secure password management software and will be trained to do so during their induction.
3. Passwords should not be saved in an unsecured location, including writing them on a piece of paper.
4. Passwords should be strong and unique passwords for each digital platform (i.e. do not re-use passwords for different accounts) and should be regularly changed to avoid risk of compromise.
5. Passwords should not use personal information that is easily guessed or publicly available (e.g. date of birth, postcode, pet names, family names).
6. In case of compromise or data leak, immediately change all passwords.
7. Staff should not share passwords with other staff unless authorised to do so by the CEO. Where passwords must be shared, this must be done through a password manager (e.g. LastPass).
8. Enable multi-factor authentication on all platforms where this functionality is available, on both personal and work devices.
9. Do not approve unexpected or unknown sign-in attempts in your multi-factor authentication application or device. If you receive such an attempt, change your password and consult with our IT provider about any other steps that should be taken.

B. Use of personal and work devices

1. Each permanent employee is to be provided with a work laptop or computer. All devices are set up using a standard user account and managed by our IT provider through administrator access.
2. All MWC devices have reputable security software installed, with at least daily updates to the signature database and a daily full scan of files.

3. All MWC devices are registered for alerts to all software updates.
4. Staff should not ignore or disable security alerts or use and/or download pirated software.
5. Staff should not run outdated or legacy software (i.e. software that is no longer updated or maintained by the developer) unless it is genuinely necessary, and only do so with close IT supervision. Software updates to work devices must be promptly installed. If you are unsure, contact our Operations Manager or IT provider.
6. When using work devices outside of the workplace, staff are prohibited from using insecure public wi-fi networks (e.g. free wi-fi in cafes, airports, or hotels).
7. Personal portable devices such as smartphones and tablets may be used to access work files (via SharePoint) and connect to the office network, intranet, emails, and communication platform (Slack). In such circumstances, staff are not permitted to download any work files onto their personal devices.
8. Staff are not permitted to use personal laptops or home computers to access, download, and work on MWC data, unless expressly permitted by the CEO.
9. When using personal devices for work purposes, staff must ensure that the device is protected by a strong PIN or password. Unprotected personal devices must never be used to access MWC data.
10. When using personal devices for work purposes, staff must ensure that reputable security software is installed on the device with at least daily updates to the signature database and a daily full scan of files, and that all software updates are promptly installed (staff must register for alerts to all software updates and promptly install them).
11. When using personal devices for work purposes, staff must ensure that they are logged out of all MWC systems before they leave the devices (e.g. log out of ActionStep before leaving the room to use the bathroom).
12. Staff must ensure that work devices and personal devices used for work purposes are physically secure (i.e. locked away) and stored safely, especially when not in use, and are never left physically unattended in a public place (even if locked or shut down).
13. Staff must ensure that work devices or personal devices used for work purposes are never left unattended while logged-in and unlocked (including in the office).

14. Remote access to our work devices is only to be used by our IT provider to provide technical assistance.

C. Use of external or removeable media devices

1. Staff should only use external or removable media devices such as USB sticks, memory cards, and external hard disks where necessary and in very limited circumstances.
2. In such circumstances, staff will need to use MWC devices and where possible only connect it to devices with anti-virus software (see paragraph 5 below) and with no access to the web.
3. Memory cards should only be used to store media files requiring large amounts of data (e.g. photos and videos), and all files should be backed up digitally to the cloud (e.g. Actionstep or SharePoint).
4. External or removeable media devices should only be used for storing presentation files to do external information sessions, or providing presentation files to partner organisations or ambassadors, where there is no other option.
5. Where possible, the removable media device must always be used with a laptop or computer that is securely equipped with an updated antivirus program, and a full antivirus scan should be run prior to using the removable media device.
6. All files stored in the removable media devices should also be digitally and securely backed up in the MWC intranet or cloud (e.g. OneDrive, SharePoint, etc.).
7. Limit the use of external or removeable media devices to store or transfer personal information or other sensitive or privileged data; and in such cases, ensure that all copies of such data are encrypted when transferring that data to other organisations (such as by using a password-protected ZIP file).
8. Do not use external or removeable media devices unless they are from the MWC or a source that you are confident is secure.

D. Secure digital culture

1. Staff (including, where appropriate, contractors) should be required to sign a code of conduct or confidentiality agreement.

2. New staff who will have access to MWC data should undertake training on data protection and digital security (including cyber security and the process for a cyber incident or data breach in section 4G of this document) as part of their induction.
3. Staff with access to MWC data should receive regular and up-to-date training on data protection and digital security (including cyber security), including practice scenarios testing that everyone is clear about what to do in the event of a cyber incident or data breach.
4. Staff should always be alert to anything unusual or suspicious, and must never open unknown or suspicious attachments or links.
5. All client information and documents must be uploaded to Actionstep, and all of staff's private work files saved to the MWC SharePoint intranet (instead of on any laptops or portable devices you may be provided).
6. Staff access to data should be restricted to data that is relevant to their role. In some circumstances (e.g. volunteers), the period and scope of access should be restricted.
7. Where personal information or other sensitive data is collected on paper, it must be converted to electronic form as soon as practicable. Paper copies must be securely destroyed (i.e. shredded). Old paper files (where digitalisation was not carried out) should be either digitalised or stored for at least 5 years before being securely destroyed.
8. Staff should not save company credit card information to any internet browser.
9. It is important for our work that our data is useful, current and accurate so it is in our best interests to ensure our data is up-to-date. Old, redundant and useless data should be deleted.

E. Regular digital security reviews

1. The Operations Manager is responsible for ensuring that the following checklist is completed:
 - a) At least once per month:
 - a. monitor for cyber security news, updates, recent issues and new cyber threats and communicate to all staff
 - b. check that no unauthorised access or breaches have occurred
 - c. review who has permission to access what data and digital platforms (e.g. ensure that access is updated as required for changed roles)

- d. send a reminder to audit staff email settings, particularly their email/forwarding rules, to ensure their emails are not being redirected without their knowledge
 - e. check that backups are being made as scheduled
- b) At least once per year:
- a. test that the backups can be successfully restored. If a backup test fails, investigate the issue and take corrective action immediately
 - b. update and test the process for a cyber incident or data breach in section 4G of this document
 - c. review IT providers, systems and processes

F. Offboarding checklist

1. The Administrative Coordinator is responsible for ensuring that the following steps are undertaken when a staff member (including directors, volunteers and students) will no longer work for the MWC:
 - a) ensure users return any office keys and MWC devices including laptops or portable devices
 - b) ensure that MWC devices and hard drives have been securely and completely erased
 - c) promptly request the IT provider to ensure that the user can no longer access all Microsoft 365 applications
 - d) promptly revoke access to any other office systems including ActionStep and other third-party applications (this will need to be done manually)
 - e) promptly revoke any temporary access and do not re-use log-in accounts for any temporary staff (e.g. “volunteer1”)

G. Process for a cyber incident or data breach

1. A “cyber incident” is an occurrence of a system, service or network state indicating a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security.
2. A “data breach” occurs when Data Protection is compromised and personal information or other sensitive data that is held by the MWC is subject to misuse, loss, unauthorised access, modification or disclosure.
3. Where staff notice a suspicious activity or suspect that a cyber incident has occurred or may occur (e.g. potential email hacking, spoofing, phishing, etc.), they must immediately:

- a) document the incident
 - b) report it to their supervisor and the CEO
 - c) contact our IT provider.
4. Other examples of a data breach could include:
- a) finding personal information or other sensitive paper information lying around at the MWC office
 - b) learning a staff member has emailed data to themselves
 - c) accidentally sending data to the wrong person.
5. If a data breach is suspected, MWC staff should:
- a) where possible, contain the breach immediately to prevent further compromise of Data Protection
 - b) document the incident
 - c) report it to their supervisor and the CEO
 - d) where the data breach was digital, contact our IT provider.
6. The CEO or their delegate will take the following actions, as appropriate or required in the circumstances:
- a) immediately take any further steps to contain the breach to prevent further compromise of Data Protection
 - b) assess the risk of harm to affected individuals by investigating circumstances of the breach
 - c) notify affected individuals
 - d) check our IT provider's response capability
 - e) review the breach and the MWC's response to consider action to prevent future incidents of a similar nature and improve the handling of future breaches
 - f) in the case of serious breaches that may involve a foreseeable risk of harm to affected individuals, or that reveal a problem in our Data Protection and Digital Security, report the incident to the Board
 - g) report the incident to the MWC insurer or funding partners, if required by our insurance policy or funding agreements
 - h) if the breach involved a breach or potential breach of the MWC's or its employed or volunteer lawyers' obligations under the legal profession laws and regulations, discuss with the MWC Principal Lawyer and/or the Board with a view to reporting to the Victorian Legal Services Board
 - i) if the breach may involve a foreseeable risk of harm to affected individuals, consider voluntary reporting to the Office of the Victorian Information Commissioner in cases of breaches involving personal information (or the Health Complaints Commissioner in cases of breaches involving health information)

- j) if the breach involved a cyber incident, consider reporting to the Australian Cyber Security Centre and the security team of any involved banks
- k) consider reporting to the Police.

Policy number	MWC Ltd Pol/08	Version	2
Drafted by	S Gayatri, G Dain & E Palmer	Last review date	March 2025
Approved by	MWC Ltd Board	Next review date	March 2026

APPENDIX 1: PRIVACY POLICY

Privacy Policy MIGRANT WORKERS CENTRE

Our obligations to your privacy

1. The Migrant Workers Centre is committed to protecting your privacy.
2. We are bound by the *Information Privacy and Data Protection Act 2014* (Vic) and the *Health Records Act 2001* (Vic).
3. These laws impose obligations on us in relation to the collection, use, disclosure and storage of personal information, including health information and sensitive information, which are types of personal information.
4. As a law practice and as lawyers, we also have professional and ethical obligations to clients of our legal service in relation to the confidentiality of their information.
5. This Policy provides an overview of how we are meeting these obligations and explains to you:
 - What personal information we collect
 - Why we collect personal information
 - How we use and disclose personal information
 - How we store and protect personal information
 - How to access and correct your personal information, or make a complaint
6. This policy concerns all personal information collected, used and stored by the Migrant Workers Centre, including information about:
 - clients, potential clients and service users of the Migrant Workers Centre
 - people working for or applying to work for the Migrant Workers Centre, including staff, directors, secondees, labour hire, contractors, students and volunteers
 - people who provide donations, goods or services to the Migrant Workers Centre.
7. Our website and email communications may contain links to other websites and social media pages including Facebook, Twitter/X, TikTok, and LinkedIn. We are not responsible for the privacy policies of the entities responsible for those websites.

What personal information we collect

Personal information is information or opinion about an individual who can reasonably be identified, whether true or not, recorded in any form.

Sensitive information is information or an opinion about an individual's:

- racial or ethnic origin
- political opinions
- religious beliefs or affiliations
- philosophical beliefs
- membership of a professional or trade association, or union
- sexual preferences or practices or
- criminal record.

Health information includes information or opinion about:

- an individual's disability
- an individual's physical, mental or psychological health
- a health service provided or to be provided to an individual
- an individual's expressed wishes about the future provision of health services to them.

8. Examples of the personal information that the Migrant Workers Centre might collect about you include:

- name, date of birth and contact details
- racial or ethnic origin
- visa or citizenship information, including year of arrival in Australia
- languages spoken, proficiency in English and need for an interpreter or translator
- gender identity and preferred pronouns
- financial information, such as your income, Centrelink benefits and housing status
- banking or payment information, if you donate or provide a good or service to the Migrant Workers Centre
- health and/or disability information, including your support needs
- family circumstances, such as number of dependent children
- LGBTQIA+ information
- union membership information
- education and employment information
- identifying numbers linked to other personal information, such as a client number or tribunal or court case number
- your internet protocol (IP) address and cookies, when interacting with our website

When and how we collect personal information

9. The Migrant Workers Centre might collect personal information (including sensitive or health information) about you when you:
 - contact us for any reason, such as to enquire about or apply for our services, or to provide feedback or make a complaint
 - become a client of our legal service and receive legal advice or assistance
 - are involved in a matter with one of our clients, including if you are supporting one of our clients or if you are another party (such as an opponent) in one of our client's legal matters
 - attend an event or activity hosted or sponsored by the Migrant Workers Centre
 - post or comment on our social media pages or complete one of our surveys
 - apply for a job or volunteer opportunity at the Migrant Workers Centre
 - provide goods or services to or on behalf of the Migrant Workers Centre.
10. The Migrant Workers Centre will almost always collect personal information about you directly from you, unless it is unreasonable or impractical to do so. We may collect personal information about you from a third party, for example if that party contacts us on your behalf or refers you to us. In that situation, we will try to speak with you directly rather than collecting information about you through a third party.
11. We only collect sensitive or health information about you if you have consented and the information is necessary for the performance of our functions, or as authorised by law.
12. For members of the public engaging with the Migrant Workers Centre, the information that we collect about you is the information that you share with us, such as your name and contact details.
13. The nature of the services offered by the Migrant Workers Centre, especially our legal service, means that it is not generally practicable to deal with individuals in an anonymous way. However, you may choose not to identify yourself or provide other information when dealing with the Migrant Workers Centre in other capacities, such as when making enquiries by phone or engaging with our social media, and not when you are a client of our legal service.

Why we collect personal information

14. The Migrant Workers Centre collects personal information for these purposes:
 - to respond to your enquiry or feedback, request for help, or application for our legal service
 - to provide you with services, such as legal advice or assistance, that are tailored to your needs

- to try to find someone else who can help you if we can't and to refer you to relevant services (but we won't share your personal information with another service without your consent)
- to manage the risks of conflicts of interest (for example, between our clients)
- to plan and design our services and activities to best meet the needs of migrant workers in Victoria
- to monitor the performance of our employees and volunteers and the quality of our services
- to recruit, train and manage staff, directors, secondees, labour hire, contractors, students and volunteers
- to source, engage and manage providers of goods and services to the Migrant Workers Centre
- to secure funding and donations and meet our obligations to our funders and donors, such as reporting obligations and accountability requirements (on an aggregate, anonymised or de-identified basis)
- to advocate for changes to the law and policy to improve rights and protections for migrant workers (for example, by using aggregated, anonymous or de-identified data, or case studies with consent)
- to communicate with you about the services that we provide, our initiatives and activities, and developments or opportunities that may be relevant to you
- to comply with our legal or contractual obligations, for example as a law practice.

How we use and disclose personal information

15. The Migrant Workers Centre only uses personal information for the purposes outlined above or for another purpose required or authorised by law.

16. We will generally only use or disclose personal information for the purpose for which it was collected, or another related purpose to which you have consented to or for which you would reasonably expect us to use or disclose it.

17. It may be necessary for us to share your personal information with:

- barristers, lawyers, experts or other persons or organisations assisting us in relation to your legal or other issues and needs. For example, we may consult with another lawyer or service for a second opinion about your issue
- other persons or organisations that the Migrant Workers Centre has contracted to provide us with services, such as information technology providers, couriers or professional advisers such as accountants, lawyers or consultants
- other institutions or parties involved in your legal matter, such as courts or tribunals, or lawyers representing other parties
- law enforcement agencies, support services or other persons or organisations if disclosure is reasonably necessary to reduce or prevent a serious threat to your life or the public's health and safety.

18. However, we will generally only disclose your personal information to someone outside of the Migrant Workers Centre with your consent, or as required or authorised by law.
19. We use contact information for the purposes of keeping in touch with our community. You can remove yourself from any mailing lists or subscriptions at any time. The way to do so will be set out in each piece of correspondence or by emailing mwc@migrantworkers.org.au.

How we store and protect personal information

20. The Migrant Workers Centre has systems in place to ensure that your personal information is stored securely on our servers and physically at our office to protect that information from misuse, loss or unauthorised access, modification and disclosure.
21. These measures include restricted access to premises, strong passworded access to computers and other devices, firewalls and anti-virus software and electronic records stored using a secure document storage system with regular back-ups.
22. The Migrant Workers Centre stores its data using third-party providers with servers located in Australia. We do not use overseas providers of information technology services including servers and cloud services.
23. We do not transfer personal information to a third-party recipient outside of Victoria unless that recipient is subject to similar obligations as Victorian privacy laws when handling that information, or you have consented.
24. The Migrant Workers Centre requires all staff, directors, secondees, labour hire workers, contractors, students and volunteers to handle personal information with care, and access only what is necessary to perform the functions of their roles.
25. In most cases, only those persons who are assisting a client, potential client or service user, or who are providing supervision or support to someone who is providing that service, will access that service user's personal and health information.
26. The Migrant Workers Centre conducts annual assessments of third-party providers to ensure security compliance standards are met.

Unique client identifiers

- 27. We create a 'unique identifier' or client number for each person who is provided with a service by the Migrant Workers Centre, including general information or referral to another service.
- 28. This system helps us to keep a record of the services provided, make appropriate referrals and avoid conflicts of interest.

How to access and correct your personal information or make a complaint

- 29. If we are assisting you with a legal or non-legal problem, we ask that you tell us when your personal information (such as contact details) changes.
- 30. You generally have the right to access any personal information that we hold about you, subject to some exceptions, such as where providing access would have an unreasonable impact on the privacy of another individual.
- 31. If you request access to your personal information held by us, we will try to provide the information to you in a timely way. If we refuse access, we will provide you with written reasons and information about available complaint mechanisms.
- 32. If you consider that the personal information that we hold about you is inaccurate, incomplete, misleading or not up to date, we will take reasonable steps to correct the information or, if we disagree that the information requires correcting, you may request that we add a note to the personal information stating that you do not agree with it.
- 33. You can make a complaint to us about how we have dealt with your personal information. We will handle your complaint confidentially and will try to resolve it in a timely, fair and reasonable way.
- 34. If you have any queries about the way we manage personal information, the personal information that we hold about you or the way we have handled your personal information, or if you'd like to request access to your information, update or correct your personal information or make a complaint, please contact the lawyer or community organiser who has assisted you, or contact us:

Migrant Workers Centre
 54 Victoria St, Carlton VIC 3053
 (03) 7009 6710
mwc@migrantworkers.org.au

- 35. For complaints about personal information that is not health information, you can make a complaint to the Office of the Victorian Information Commissioner if you do not receive a response from us within 28 days, or if you are unsatisfied with how we

dealt with your complaint. Further general information about privacy is available on the website of the Commissioner at www.ovic.gov.au or by calling the enquiry line at 1300 006 842.

36. If your complaint is about health information, you should direct your complaint to the Health Complaints Commissioner via their website hcc.vic.gov.au or call 1300 582 113.

Clients and prospective clients of our legal service

37. For clients and prospective clients of our legal service, we collect information about you and your legal problem to:

- decide whether we can provide you with legal help
- provide you with legal help tailored to your needs and circumstances
- try to find someone else who can help you if we can't (we won't share your personal information with another service without your consent).

38. For example:

- We ask about what country you were born in and where you live and work, because our legal service is only available to persons who were born overseas who live or work in Victoria
- We ask for the names of other people involved in your case because, lawyers are not allowed to act for a client if there is a conflict of interest with another current or former client
- We ask about whether you are a union member so that we can help you to access services from your union, or to join a union if you want to
- We ask about things like whether you require an interpreter or have any disability support needs so that we can tailor our service to your needs
- We ask about things like your financial and family circumstances so that we can prioritise assisting clients who need our help the most, and so that we can try to find services to assist you with other things you may need, such as finding accommodation or accessing financial counselling.

39. If you do not provide us with the information that we request, we may not be able to provide you with help, or the help that we provide may not be appropriate to your needs and circumstances.

40. For clients of our legal service, our use and disclosure of your information is also governed by our obligations as a law practice and as lawyers. For example:

- A lawyer must not disclose any information that is confidential to a client without their authorisation, subject to exceptions such as to prevent imminent serious physical harm to the client or another person.
- We are required to allocate a unique identifier or file number to each legal file.
- We are generally obliged to keep a copy of your file for seven years after it is closed. We will try to return any of your original documents to you before closing your file. After seven years, we will destroy all copies of legal files unless there are circumstances that warrant a longer retention period.

41. In addition to the complaint mechanisms set out above under ‘How to access and correct your personal information or make a complaint’, complaints about lawyers can be made to the Victorian Legal Services Board and Commissioner. For more information, visit www.lsbc.vic.gov.au.

Our website

42. The Migrant Workers Centre website is hosted by a third-party platform, which advises that it may use automatic data collection technologies to collect information about your equipment, browsing actions and patterns, including:

- device and usage information, which may include the type of device you are using, your operating system, your browser type, your browser language, your internet service provider, your domain name, your IP address, your device and mobile ad identifiers, the website that referred you to our website, the web pages you view (including the date and time you viewed them), the services or functionality you access or use (including the date and time of your access or use)
- location information (which may include general information about the location of your device based on your IP address)
- in some cases, click or touch stream data, movement, scroll, and third-party sites or services you were using before and after interacting with our services.

43. Cookies may be used on our website. A ‘cookie’ assists us to understand how visitors to our website use it and to make assumptions about what information may be of most interest to visitors to our website. Cookies may be used, stored and analysed in our IT systems and by our server and network hosts. It is possible that personal information will be captured in those processes. You will usually find information on cookies, and how to manage them, under ‘Options’ or ‘Settings’ on your browser. For more information about managing cookies, see the guidance from the Office of the Australian Information Commissioner (oaic.gov.au).