Approved by:	CEO
Approved date:	February 2024
Date for review:	February 2026
Review frequency:	Biennially
Version:	2.1

Privacy Policy

Policy Number 3.14.

KNOWLEDGE AND INFORMATION MANAGEMENT

1. Background

Privacy is a key principle that underpins Wentworth Healthcare's collection of personal information - what personal information is collected and why. It is an underlying principle in all our practices, procedures, and systems.

In undertaking the collection of personal information, Wentworth Healthcare complies with The Privacy Act 1988 (Privacy Act). The Privacy Act was introduced to promote and protect the privacy of individuals and to regulate how Australian Government agencies and organisations handle personal information.

The Privacy Act defines **personal information** as:

…information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable

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

Personal information includes a broad range of information, or an opinion, that could identify an individual. What is personal information will vary, depending on whether a person can be identified or is reasonably identifiable in the circumstances. Personal information is not limited to information about an individual's private or family life, but extends to any information about or opinions of an individual, from which they are reasonably identifiable. This can include information about an individual's business or work activities. Personal information can range from sensitive and confidential information to information that is publicly available.

The Privacy Act also includes 13 Australian Privacy Principles (APPs). The APPs are the cornerstone of the privacy protection framework in the Privacy Act, governing standards, rights and obligations around:

- the collection, use and disclosure of personal information;
- an organisation or agency's governance and accountability;
- integrity and correction of personal information and;
- the rights of individuals to access their personal information.

A breach of an Australian Privacy Principle is an 'interference with the privacy of an individual' and can lead to regulatory action and penalties.

The Privacy Act also regulates the privacy component of the consumer credit reporting system, tax file numbers, and health and medical research.

2. Purpose

The purpose of this policy is to clearly express how Wentworth Healthcare currently manages personal information it collects and to make this explanation readily available to Wentworth Healthcare staff through this policy and accompanying procedures and to the public through our website.

3. Scope/Application

This Privacy Policy broadly defines how Wentworth Healthcare manages the personal information it collects, and the information flows associated with that personal information.

This policy applies to all forms of personal information handling and the practices, procedures and systems of our organisation to ensure an open and transparent approach is applied. The accompanying procedure provides related information of how information management practices in line with Privacy legislation is implemented within Wentworth Healthcare.

Key areas of scope that importantly align to the APPs include:

3.1 Kinds of personal information collected and held

Wentworth Healthcare considers the need to collect and retain personal information as a first step. Personal information is only held for a specific purpose in order to carry out functions or activities. The security of this information is maintained for its entire lifecycle. This includes:

- Personal information and some sensitive information on all **employees**. This information forms a part of an employment record and is a necessary part of the employment process. This may also include some sensitive information.
- To assist us in meeting our contractual obligations, Wentworth Healthcare may collect personal information from **key stakeholders** with whom we work such as healthcare professionals and practice staff, commissioned service providers, committee members, community members, NGOs and other health and non-health agencies.
- A limited amount of personal information from all **visitors and contractors** entering Wentworth Healthcare premises primarily in support of Work Health Safety requirements.

3.2 How personal information is collected and held

Wentworth Healthcare takes reasonable steps to protect this information from **misuse, interference and loss**, as well as **unauthorised access, modification or disclosure**. Wentworth Healthcare also takes reasonable steps to destroy or de-identify personal information held once it is no longer needed.

3.3 All personal information is collected directly, and through an informed consent process. The information is then held securely for the duration of its specific purpose and in line with legislative requirements for document retention as set out in the Wentworth Healthcare Data Access, Collection, Retention, Archive and Disposal Policy. Purposes for which the entity collects, holds, uses and discloses personal information.

Any personal or sensitive information collected, held, used and or disclosed by Wentworth Healthcare to a third party is undertaken for a specific purpose and with the express consent of those engaged in the process with Wentworth Healthcare including:

- Collection of personal and sensitive information on Wentworth Healthcare staff forms part of the specific employment process.
- Collection of personal information from key stakeholders is to support Wentworth Healthcare to fulfil its contractual and/or legal obligations.
- Collection of personal information for visitors and contractors entering Wentworth Healthcare premises is to support work health and safety.
- Collection of personal information from other entities, including those Wentworth Healthcare may commission to deliver a service, is a part of a formal service contract or agreement.

3.4 Unsolicited information

Unsolicited personal information is provided without it being requested. If Wentworth Healthcare receives unsolicited personal information about an individual from other individuals or entities, without it being requested, it will be handled the way other personal information is handled by Wentworth Healthcare, in accordance with the APPs. The information will be destroyed as soon as practicable and the sender will be notified.

3.5 Accessing and seeking correction of personal information

Wentworth Healthcare maintains procedures to enable individuals reasonable access to their personal information and, as appropriate, the ability to correct, delete or update inaccurate or incomplete information.

Whilst all Wentworth Healthcare staff are bound by the legal requirements of the Privacy Act and the APPs relating to information access and correction, the Privacy Act operates alongside and does not replace other informal or legal procedures by which an individual can be provided with access to, or correction of, their personal information, including the *Freedom of Information Act 1982* (FOI Act).

All individuals have a right to request access to the personal information Wentworth Healthcare holds about them. If an individual makes a request to access their personal information, Wentworth Healthcare will ask the individual to verify their identity and specify the information they require. Further, if an individual considers that the personal information Wentworth Healthcare holds about them is inaccurate or contains inaccurate information, they can request an amendment to their personal information.

All requests can be made in writing, marked to the attention of the Privacy Officer and submitted as follows:

Email: privacy@nbmphn.com.au Postal address: Wentworth Healthcare,

Blg BR, Level 1, Suite 1,

Locked Bag 1797,

Penrith NSW 2751

Phone: (02) 4708 8100

Requests will be acknowledged within seven days, and the intent is to respond to all requests within 30 days from the original request date.

Subject to the APPs, Wentworth Healthcare may deny individuals access to their personal information in the following situations:

- the information relates to existing or anticipated legal proceedings between the individual about whom the information relates and ourselves, and would not be accessible by the process of discovery in those proceedings;
- access would reveal our intentions in relation to negotiations with the individual in such a way as to prejudice those negotiations;
- granting access would be unlawful; or
- giving access would be likely to prejudice the taking of appropriate action in relation to the matter.

If access to personal information is refused in accordance with the APPs, a written notice will be provided to identify:

- the reasons for denying access to personal information (except where it would be unreasonable to provide the reasons);
- the mechanisms available to complain about the refusal; and
- any other matters prescribed by the regulations.

3.6 Complaints about a breach of the APPs

Wentworth Healthcare is committed to taking all complaints seriously and recognises and respects everybody's right to provide feedback or lodge a complaint about a breach of the Australian Privacy Principles. All complaints are treated fairly, with impartiality and transparency, while maintaining confidentiality.

Mechanisms are in place to receive, consider and resolve complaints related to privacy breach in a timely and effective manner. All assessment of complaints will be undertaken in a manner consistent with our values and code of conduct.

Where a privacy related complaint is received regarding a service Wentworth Healthcare commissions or delivers, Wentworth Healthcare will address the complaint and will expect the subcontracted service provider to have an accessible and comprehensive privacy complaint management system in place.

Further details about the complaints process, including dispute resolution, can be found within the accompanying procedure and on our NBMPHN website within 'Have your say'.

3.7 Overseas disclosures

Wentworth Healthcare's preference is to retain all personal information within Australia and in the majority of circumstances will not disclose personal information to overseas recipients. In the event that personal information is collected and that the personal information is likely to be disclosed to overseas recipients (for example, the use of a survey platform where the host server is located overseas), individuals will be notified of the location of those recipients, and informed consent will be obtained prior to this progressing.

Wentworth Healthcare will only transfer personal information about an individual to someone who is in another State or foreign country if:

- Wentworth Healthcare is reasonably sure that the information will not be held, used or disclosed inconsistently with the privacy principles set out in the Privacy Act; or
- the recipient is bound by legislation that is substantially similar to the Privacy Act.

3.8 Exemptions and specific obligations

There are no exemptions or specific obligations that apply to Wentworth Healthcare under the Privacy Act relating to personal information held by Wentworth Healthcare or to any of our acts or practices.

3.9 Anonymity and Pseudonymity

Where it is lawful and practicable to do so, Wentworth Healthcare will allow individuals to interact with the organisation and provide information anonymously or through the use of a pseudonym.

This includes (but is not limited to):

- submitting feedback or complaints anonymously or using a pseudonym;
- contacting the organisation and requesting information via phone, email, mail or online without being required to provide identifying information; and
- completing surveys without providing identifying information.

Staff will ensure that individuals are aware of any potential consequences resulting from their decision of anonymity including the ability of Wentworth Healthcare to interact and provide feedback with the individual will be affected.

Anonymity will generally not be possible in all circumstances for our employees, contractors and commissioned service providers.

3.10 Direct Marketing

Wentworth Healthcare provides its members and stakeholders with information about its activities through a number of communication mechanisms including newsletters and event invitations. In accordance with the *Spam Act 2003*, any direct marketing activity will be consent-based and individuals and organisations receiving such information will be provided with the opportunity to unsubscribe.

3.11 Quality of Personal Information

Wentworth Healthcare will take all reasonable steps to ensure that personal information that is kept, used or disclosed is accurate, complete and up to date as practicable in line with our Data Quality Policy and Procedures; and Data Access, Collection, Retention, Archive and Disposal Policy.

Consumers and stakeholders are invited to contact us if they become aware that the information we hold on them is inaccurate or out of date.

3.12 Transferring information to Wentworth Healthcare online

There are risks in transmitting information across the internet. Wentworth Healthcare cannot ensure the security of information transmitted via on-line channels. It should be noted that once personal information is received, Wentworth Healthcare takes reasonable steps to protect that information from misuse, loss, unauthorised access, modification and disclosure are in accordance with this privacy policy. Stakeholders are encouraged if they have concerns about conveying personal and or sensitive material to Wentworth Healthcare over the internet, to use other methods such as telephone, mail or in person.

Wentworth Healthcare's website uses cookies and web beacons. A cookie is a small piece of code that is placed on your computer. A web beacon is a piece of code that is placed on each page that communicates the cookie's content once the page is visited.

Cookies and web beacons may collect the information about each page of the website visited, the server address, the type of browser being used, the operating system, the top level domain name and the date and time that each page is accessed. Wentworth Healthcare uses Google Analytics to monitor website activity, and some of these features may include non-identifiable demographic information.

Use of cookies and web-beacons does not involve the retrieval or recording of any personal information (such as a name or email address). To the extent that this data could make an individual identifiable, attempts will not be made to identify an individual from these records. The information is used for the purpose of website management and development only. Visitors are able to prevent their data from being used by Google Analytics through opt-out applications, such as the Google Analytics Opt-Out Browser Add-On.

Individuals may be required to log in to a Wentworth Healthcare website in order to access certain functions. In this instance, website visitation activity will be personally identifiable, however this data is only used to maintain the website services offered by Wentworth Healthcare and understand how they can be improved.

The Wentworth Healthcare privacy policy does not apply to, and Wentworth Healthcare is not responsible for, the use of, or the protection of information provided to, other websites linked to through Wentworth Healthcare's websites. By providing a link to another website, Wentworth Healthcare is also not endorsing that website nor guaranteeing the accuracy of the information contained on that website.

4. Privacy Framework

Wentworth Healthcare has developed a four-step framework to support the implementation of privacy that includes:

Step 1: Embedding a culture of privacy that enables compliance

Wentworth Healthcare's leadership and governance arrangements creates a culture of privacy that values personal information.

Step 2: Establish: **Robust and effective privacy practices, procedures and systems**

Wentworth Healthcare has effective practices, procedures and systems to support good privacy management.

Step 3: Continuous Improvement

Wentworth Healthcare regularly evaluates privacy practices, procedures and systems to ensure continued effectiveness.

Step 4: Enhancing Wentworth Healthcare's response to privacy issues

Wentworth Healthcare is committed to ensuring responsiveness to new privacy issues.

5. Policy Statement and Principles

Wentworth Healthcare is committed to ensuring an individual's privacy is protected by meeting our obligations under the *Privacy Act 1988*. In confirming our obligations under the Privacy Act, Wentworth Healthcare has made a leadership commitment to foster a culture of privacy as the foundation for good privacy governance. Good privacy governance will also help Wentworth Healthcare to manage both the risk of a privacy breach and a response should one occur.

Wentworth Healthcare will take reasonable steps to implement practices, procedures and systems that will manage personal information in an open and transparent way. In doing so, it is important that community trust and confidence are maintained which is exemplified by the way we uphold our privacy obligations. By embedding a culture that respects privacy, Wentworth Healthcare builds a reputation for strong and effective privacy management that will inspire trust and confidence with our community.

Wentworth Healthcare in defining the **guiding principles** that support our implementation of privacy, have taken into consideration the objects of the Privacy Act 1988 that incorporate:

- Promoting the protection of individual's privacy;
- Appling consistency with the privacy handling of personal information;
- Ensuring responsible and transparent handling is applied with all personal information;
- Recognising protection of an individual's privacy is balanced with carrying out Wentworth Healthcare's functions and activities;
- Facilitating the flow of information where and when required whilst ensuring an individual's privacy is respected; and
- Enabling the means for individual's to complain about alleged interference with their privacy.

Based on the Company's Risk Appetite Statement, Wentworth Healthcare has assessed **Privacy risk** as a 'Controlled' risk in respect to the Regularity area and 'Cautious' in respect to Governance. This means that is a **zero to low** tolerance for Privacy risk.

Furthermore, *Data security and privacy protection* is one of 5 key data governance concepts that underpin Wentworth Healthcare's Data Governance Framework and approach to risk. As such, Wentworth Healthcare is aware of and seeks to uphold, the high standards that the community and stakeholders expect. This has been realised through the implementation of a Privacy Impact Assessment (PIA) Policy and Procedure that assists with the assessment of risk.

Wentworth Healthcare's Board, Executive, Managers, Staff, Commissioned Service Providers and Key Stakeholders are supported to have an understanding of, and access to, the Wentworth Healthcare Privacy Policy, PIA Policy and other related procedures, forms and guidelines.

6. Roles and Responsibilities

The **Wentworth Healthcare Board** has ultimate responsibility for both accountability and responsibility for ensuring that privacy obligations in protecting an individual's privacy under the Privacy Act 1988 are met. Although the Board has ultimate accountability, implementing privacy is the responsibility of all staff.

- The Board has appointed the **CEO** to provide oversight of Privacy policy and management. The **CEO and Executive** have a responsibility to implement Privacy systems within the organisation. Where the implementation is delegated, a system of monitoring is in place that provides a mechanism to confirm that the security of personal information is protected.
- The actions and decisions of the CEO and Executive in relation to Privacy is informed and supported by **Committees** including the Board Finance and Audit Risk Management Committee, Board Clinical Governance Committee and Management's Data Governance Committee.
- Wentworth Healthcare **Managers and their staff** are responsible for understanding, utilising and implementing Wentworth Healthcare's privacy policy and for overseeing the day-to-day implementation of privacy systems in their respective program areas of responsibility.

Key appointments that support both the CEO to discharge privacy responsibilities and monitor organisational compliance are:

- The **Privacy Officer**, performed by the position of Executive Manager Strategy and Integration, is the first point of contact for advice on privacy matters for Wentworth Healthcare staff.

  The Privacy Officer plays a vital role in promoting strong privacy governance and capability within Wentworth Healthcare to support compliance with the Code. This helps to build public confidence that Wentworth Healthcare is respecting and protecting personal information. The Privacy Officer will need to have:

  - An in-depth understanding of the Privacy Act and the Code, and the ability to translate these requirements into practice within Wentworth Healthcare.
  - An understanding of any other legislation that governs the way Wentworth Healthcare handles personal information.
  - The ability to understand Wentworth Healthcare's strategic priorities and key projects involving the use of personal information.
  - An understanding of the systems and processes Wentworth Healthcare uses to handle personal information.
  - An understanding of privacy dispute resolution and complaint-handling methods and processes.

  The functions performed by the Privacy Officer, which may also be performed by another person (or persons) required under the Code include:

  - Providing privacy advice internally on:
    - The development of new initiatives that have a potential privacy impact.
    - The general application of privacy law to Wentworth Healthcare's activities.
    - What to consider when deciding whether or not to carry out a PIA or Dataset PIA.
    - What safeguards to apply to mitigate any risks to the privacy of individuals.
  - Liaising with the Office of the Australian Information Commissioner (OAIC).
  - Co-ordinating the handling of internal and external privacy enquiries, privacy

complaints, and requests for access to, and correction of, personal information.

- Maintaining a record of Wentworth Healthcare's personal information holdings.
- Assisting with the preparation of PIAs and Dataset PIAs.
- Measuring and documenting Wentworth Healthcare's performance against its privacy management plan.
- Coordinating privacy training to agency staff.
- Proactively monitoring compliance and managing the Wentworth Healthcare's response to data breaches.

- The **Chief Data Officer**, performed by the position of Executive Manager Strategy and Integration has ultimate accountability for the primary health care data within their PHN, and for decisions related to data including the privacy protection of the same data.
- The nominated **Data Sponsors** and **Data Custodians** and all **Data Users** are also responsible for taking reasonable steps to protect the privacy of any personal information from inappropriate or unauthorised use, access or disclosure.
- **Commissioned Service Providers** are responsible for abiding by Wentworth Healthcare's Privacy Policy in situations that impact on the services and activities commissioned involving personal information of clients or patients. Obligations will be articulated clearly in communications, notices and service agreements where applicable.
- **Stakeholders and Visitors** will have access via our website, to Wentworth Healthcare's Privacy Policy that will support how Wentworth Healthcare's privacy is applied in situations that involve their personal information.

7. Definitions

Title	Definition
Australian Privacy Principles (APPs)	The APPs are legally binding principles which are the cornerstone of the privacy protection framework in the Privacy Act 1988. The APPs set out standards, rights and obligations in relation to handling, holding, accessing and correcting personal information. They apply to most Australian Government agencies and some private sector organisations - collectively referred to as APP entities. The APP provides flexibility to tailor an entities personal information handling practices to their diverse needs and business models, and to the diverse needs of individuals. The APPs are also technology neutral, applying equally to paper-based and digital environments. This is intended to preserve their relevance and applicability, in a context of continually changing and emerging technologies.
Code	A privacy code of practice is a legal instrument which allows a public sector agency or organisation to make changes to an Information Protection Principle (IPP) or provisions that deal with public registers, specify how that rule will apply in a particular situation. The Australian Government Agencies Privacy Code (the Code) was registered on 27 October 2017 and commenced on 1 July 2018. The Code applies to all Australian Government agencies subject to the Privacy Act 1988 (the Act) (except for Ministers). It is a binding legislative instrument under the Act.

	The Code sets out specific requirements and key practical steps that agencies must take as part of complying with Australian Privacy Principle 1.2 (APP 1.2). It requires agencies to move towards a best practice approach to privacy governance to help build a consistent, high standard of personal information management across all Australian Government agencies. The Code enhances existing privacy capability within agencies, builds greater transparency in information handling practices, and fosters a culture of respect for privacy and the value of personal information. The Code therefore symbolises the commitment of Australian Government agencies to the protection of privacy, and helps build public trust and confidence in personal information handling practices and new uses of data proposed by agencies.
Collection	The concept of 'collection' applies broadly, and includes gathering, acquiring or obtaining personal information from any source and by any means, including from: • individuals • other entities • generally available publications • surveillance cameras, where an individual is identifiable or reasonably identifiable • information associated with web browsing, such as personal information collected by cookies • biometric technology, such as voice or facial recognition
Consent	Consent means 'express consent or implied consent' (s 6(1)). The four key elements of consent are: • the individual is adequately informed before giving consent • the individual gives consent voluntarily • the consent is current and specific, and • the individual has the capacity to understand and communicate their consent Express consent is given explicitly, either orally or in writing. This could include a handwritten signature, an oral statement, or use of an electronic medium or voice signature to signify agreement. Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the APP entity.
Disclosure	When personal information is made accessible or visible to others outside the entity. The entity also releases the subsequent handling of the personal information from its effective control.

Employee Record	A record of personal information relating to the employment of the employee. Examples of personal information relating to the employment of the employee are personal information about all of any of the following: • the terms and conditions of employment of the employee; • the engagement, training, disciplining or resignation or the employee; • the employee's personal and emergency contact details; • the employee's hours of employment; • the employee's salary or wages; • the employee's membership of a professional or trade association; • the employee's recreation, long service, sick, personal, maternity, paternity or other leave; • the employee's taxation, banking or superannuation affairs; • the employee's performance or conduct; • the termination of the employment of the employee; • and health information about the employee (such as employer provided vaccinations).
Health Information	Information or an opinion, that also constitutes personal information, about: • the health or disability (at any time) of an individual; or • an individual's expressed wishes about the future provision of health services to him or her; or • a health service provided, or to be provided, to an individual; that is also personal information; or • other personal information collected to provide, or in providing, a health service; or • other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or • genetic information about an individual in a form that is, or could be, predictive of the health of the individual or genetic relative of the individual or a genetic relative of the individual.
Non-personal Information	Information that is confidential or commercial in nature. Often refers to information about an organisation or entity.
Personal Information	The Privacy Act defines personal information as: *…information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.* • whether the information or opinion is true or not; and • whether the information or opinion is recorded in a material form or not.' The definition is technologically neutral to ensure sufficient flexibility to encompass changes in information-handling practices over time. The term 'personal information' encompasses a broad range of information that includes:

	• Sensitive information - information or opinion about an individual's racial or ethnic origin, political opinion, religious beliefs, sexual orientation or criminal record, provided the information or opinion otherwise meets the definition of personal information • Health information' - which is also 'sensitive information' • Credit information • Employee record information • Tax file number information. Common examples are an individual's name, signature, address, telephone number, date of birth, medical records, bank account details and commentary or opinion about a person. Personal information is not limited to information about an individual's private or family life, but extends to any information or opinion that is about the individual, from which they are reasonably identifiable. This can include information about an individual's business or work activities. Personal information can range from sensitive and confidential information to information that is publicly available.
Record	The term 'record' includes a document or an electronic or other device. Some items are excluded from the definition, such as anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition, and Commonwealth records in the open access period.
Sensitive Information	Information or an opinion (that is also personal information) about an individual's: • racial or ethnic origin; or • political opinions; or • membership of a political association; or • religious beliefs or affiliations; or • philosophical beliefs; or • membership of a professional or trade association; or • membership of a trade union; or • sexual orientation or practices, or • criminal record; or that is also personal information; or • health information about an individual; or • genetic information (that is not otherwise health information); or • biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or • biometric templates.
Spam Act	Means the Spam Act 2003 (Spam Act), which is managed by the Australian Communications and Media Authority (ACMA).
The Act	Means The Privacy Act 1988

8. References and Other Documents

Document Number	Document Name	Access point
3.06.01	Privacy Impact Assessment Procedure	Intranet
3.06.01.05	PIA Threshold Assessment Form	Intranet
	WHL Privacy Impact Assessment Report	Data team
NA	PIA Process Flowchart	Intranet
	WHL Privacy Impact Assessment Register	Data team
3.06.01.04	PIA Action Plan	Intranet
	WHL Dataset PIA Tool	Data team
3.06.01.02	Dataset PIA Guidelines	Intranet
	WHL Dataset PIAs Register	Data team
3.05	Data Breach Response Policy	Intranet
3.05.01	Data Breach Response Procedure	Intranet
3.05.01.01	Data Breach Response Guidelines	Intranet
3.02.05	Data Quality Policy	Intranet
3.02.06	Data Quality Procedure	Intranet
3.03	Data Access, Collection, Retention, Archive & Disposal Policy	Intranet
	WHL Data Asset Register	Data Team
	Wentworth Healthcare Data Sharing Agreements Register	Health Data Officer
1.11	Wentworth Healthcare Risk Management Policy	Intranet

OIAC and other resources:

- The Privacy Act 1988
- Spam Act 2003
- OAIC Resources

9. Further Assistance

If you would like further information on our privacy policy, or if you have any concerns over the protection of your personal information, please contact our Privacy Officer as follows:

Email: privacy@nbmphn.com.au

Postal address: Wentworth Healthcare,
Blg BR, Level 1, Suite 1,
Locked Bag 1797,
Penrith NSW 2751

Phone: (02) 4708 8100

10. Revisions Made to this Policy

Date	Major, Minor or Editorial Revision	Description of Revision	Author
30.11.2020	Revision		Elisa Manley
1/3/21	Editorial	Proofing and Formatting	Project Support Officer Business Improvement
15/4/21	Editorial	Corrected proofing errors	Project Support Officer Business Improvement
14/02/2024	Editorial	Updating and proofing	Elisa Manley Carolyn Townsend