Code of Conduct Standard

Contents

Overview

Overarching Policy	This Standard supports the Code of Conduct Policy.
Purpose	This document defines the expected standards of behaviour and conduct required of all personnel of The Salvation Army (TSA) and anyone who engages with TSA.
Who does this apply to?	This Standard applies to all TSA personnel and anyone who engages with TSA.
Effective date	16/04/2025

Standard Statement

Principles

Expectation

The behaviour and conduct of personnel must be aligned to TSA's vision, mission and values.

It is the responsibility of personnel to be familiar with, understand and abide by the standards defined in this document.

Equal opportunity

Personnel must never act in a discriminatory way towards others.

See the definition of discrimination.

Behaviours not defined

The absence of any reference to a particular behaviour or conduct does not imply that it is acceptable.

However, a good guide is to consider whether a reasonable person would consider that behaviour or conduct to be appropriate or inappropriate.

Personal Behaviour

Integrity, honesty and respect

Personnel will:

- Conduct themselves with integrity, honesty and transparency at all times
- Treat all people with respect, dignity, fairness and courtesy
- Treat all people in a manner that conveys their worth as individuals
- Respect the opinions and beliefs of all people and the right of each person to practice their own beliefs
- Demonstrate professionalism and courtesy in dealing with other people

Dress and appearance

Personnel are required to dress in a neat, clean and appropriate manner for the particular area in which they work.

TSA supports personnel to dress in a manner that reflects their cultural, faith and / or gender identity.

Examples of Acceptable Dress	Examples of Unacceptable Dress
▪ Trousers, business shorts, pants, skirts, dresses ▪ Modest shirts, blouses, jumpers, cardigans, sports jackets ▪ Plain sports shoes in good condition	▪ Leggings, sports shorts ▪ Scruffy sports shoes, thongs, slippers, worn out footwear or similar ▪ Athletic wear (including sportswear with large brand names or motifs) ▪ Torn or ripped clothing ▪ Jewellery or accessories that may compromise hygiene and safety

Variations to the dress code that may be required based on a program, location or individual circumstances are to be approved by the appropriate Senior TSA Representative.

TSA uniform

Officers must wear TSA uniform in accordance with the Uniform and Styles Guidelines stipulated in the Active Officer Service Conditions and Uniform Policy.

TSA- Branded clothing

Personnel who wear TSA-branded clothing represent TSA and therefore must uphold the values of TSA.

Personnel are only permitted to wear TSA branded clothing during official work and volunteering activities. Personnel are permitted to wear branded clothing whilst travelling from their place of residence to and from these activities.

Personnel are not permitted to consume alcohol or smoke a cigarette in public while wearing TSA-branded clothing. Please refer to the TSA-Branded Clothing Guidelines for more information.

Personal best

Personnel are required to perform their defined duties to the best of their ability while maintaining the expected standards of behaviour and conduct.

Sensitive language

Personnel will ensure that their use of language, both written and verbal, does not make assumptions, deliberately cause offence or discriminate on the basis of an individual's:

- Cultural background
- Age
- Disability
- Religious belief
- Family status
- Gender identity or expression
- Intersex status
- Sexual orientation
- Social or economic background

Attendance and punctuality

Personnel are required to be punctual and regular in attendance and promptly notify their line manager of any unplanned absence.

Unacceptable Behaviour

Violence and assault

TSA has zero tolerance to all forms of abuse, neglect, harm or risk of harm. Personnel must not behave in any way that may be considered violent or aggressive or that may constitute assault in any form or manifestation.

Language and verbal abuse

Personnel must not use language that is:

- Abusive, rude, insulting or obscene
- Intended to harm, abuse, bully, harass, shame, humiliate, belittle or degrade
- Inappropriate, offensive or discriminatory
- Discriminatory against Aboriginal and Torres Strait Islanders, LGBTIQA+ people, people with disabilities or Culturally Diverse people

Boundaries

Personnel should not, of their own volition or at the request of a child or vulnerable adult or participant, act outside of their professional boundaries and prescribed duties (as specified in the relevant Brief of Appointment, Position Description or Role Profile).

In order to ensure supportive and safe engagement and interactions, all interactions with people must not violate their physical, psychological, religious, cultural or sexual boundary limits.

Personnel must not seek to obtain or use TSA data or service information/ knowledge to gain access to a child, vulnerable adult or participant.

Personnel with a pre-existing relationship with a child, vulnerable adult or participant must declare the relationship in accordance with this Standard (See Relationships with Clients/ Participants).

Act and report concern

Personnel must report all concerns and, complaints including any allegations of abuse, neglect, harm or risk of harm, and all actual or perceived breaches of TSA's policies relating to the safety and wellbeing of any individual, to the relevant statutory authority and a Senior TSA Representative, as soon as practicable.

Sexual misconduct and grooming

Under no circumstances is any form of sexual behaviour to occur between, with or in the presence of children or vulnerable adults, irrespective of the age of the child or vulnerable adult. This includes but is not limited to 'contact behaviour', such as sexual intercourse, sexual penetration, kissing, fondling, inappropriate touching, or 'non-contact behaviour' such as flirting, sexual innuendo, conversations (through any medium), comments about an area of the body (if these could be perceived as being for sexual gratification and not for an authorised purpose), inappropriate photography or exposure to pornography or nudity, exposure to sexual activity by others, undressing or watching someone else undress.

Any behaviour that amounts to sexual exploitation- exploiting the vulnerable situation of a person for sexual purposes to profit monetarily, socially or politically- is unacceptable. The exchange of money, employment, goods or services for sex, including sexual favours or other forms of exploitative behaviour is prohibited.

Any behaviour regarded as 'grooming', either of a child or/vulnerable adult or of another adult (an individual), with the purpose of gaining access to that individual for sexual contact and/or exploitation is a crime under Australian law and will be dealt with accordingly. It is also unacceptable and will be considered a breach of this Code of Conduct Standards, whether or not charges or convictions ensue.

Exploitation

Personnel shall not seek the influence of any person to obtain promotion or other advantage.

Personnel must not exercise any undue influence (whether physical or psychological) over any person including other staff members and clients for personal benefit or for the benefit of TSA.

Working with Children and Vulnerable Adults Guidelines

Working with children/working with vulnerable persons checks

Personnel engaged in any child related work and/or other vulnerable persons must hold a valid Working with Children Check/ equivalent (WWCC) in the relevant state or territory in which they work.

TSA personnel must immediately disclose all charges, convictions and other outcomes of an offence that relates to child exploitation and abuse. Furthermore, TSA personnel must disclose any other offences that a reasonable person would consider would bring into question the suitability of the TSA personnel to continue to work with children or vulnerable adults.

Power imbalance

Personnel are required to be aware that children and vulnerable adults often have limited or no power or voice in their relationships with others.

Personnel will ensure their behaviour recognises and minimises any power imbalance inherent in their role and position within TSA and will not take advantage of any other individual.

Relationships with clients/participants

TSA personnel must not use the position of trust they occupy to start any form of improper personal relationship within or outside the boundaries of the role. Doing so is strictly prohibited and may in fact amount to an offence under the law.

In all cases, personal relationships with clients are considered exploitative, an abuse of the power imbalance described earlier and are a breach of professional boundaries and the Code of Conduct Standards.

It is also not a defence to claim that a personal relationship with a client occurred unwittingly or that it was consensual.

Personal relationships which are pre-existing between a member of TSA personnel and clients/ participants engaged in a TSA program, must be declared each and every time the client/participant commences engagement with any TSA program. The declaration must be made by TSA personnel as soon as they become aware that a client/ participant has a pre-existing relationship with someone who is engaged or re-engaged in the program/ service that they operate in.

Where the pre-existing relationship involves children, personnel must conduct themselves in accordance with the Working with Children and Vulnerable Adults Guidelines. Any transport, child minding or overnight stays are to occur only with the written authorisation of the parent/guardian and the written authorisation of the appropriate Senior leader.

Failure to make such a declaration is a breach of the Code of Conduct.


See the Conflict of Interest Procedure and Conflict of Interest Disclosure Form.

Reporting obligations

Personnel must ensure the safety of all individuals they come into contact with, by taking immediate and appropriate action to remove, or if this is not possible, to reduce, the risk to a child or vulnerable adult. This may include immediate notification of actual or suspected harm, risk of harm, exploitation or abuse, to a Senior TSA Representative, the Police if a crime is suspected, and the relevant statutory authority.

Personnel are required to make a report immediately (i.e. as soon as practicable and no later than the end of the same day) if they:

- Become aware of any allegation(s) of abuse, neglect, harm or risk of harm and/or exploitation of a child or vulnerable adult
- Have a concern for the safety of any child/vulnerable adult in a TSA service/program
- Become aware of any personnel whose practice or behaviour is contrary to the expectations of behaviour set out in this Code of Conduct Standard and the Code of Conduct Policy.

Where any abuse, neglect, harm, risk of harm or exploitation is suspected, personnel must advise their line manager or Senior TSA representative, and proceed in accordance with TSA's Incident Management Policy and TSA's Responding to Safeguarding Concerns Procedure and all other related processes and procedures.

TSA personnel must immediately disclose all charges, convictions and other outcomes of an offence that relates to child exploitation and abuse. Furthermore, TSA personnel must disclose any other offences that a reasonable person would consider would bring into question the suitability of the TSA personnel to continue to work with children or vulnerable adults.

Physical contact

Any physical contact with children and/or vulnerable adults by personnel must be appropriate to the delivery of services and based on the needs of the child or vulnerable adult (such as to assist or comfort a distressed child/vulnerable person).

Under no circumstances should personnel have contact with a child or vulnerable adult that:

- Involves touching of genitals, buttocks or breast area, other than for the purposes of delivering medical, allied health or personal care services to the child or vulnerable adult
- Causes pain or distress to the child or vulnerable adult, e.g. corporal punishment
- Is overly physical, including, but not limited to wrestling, horseplay, tickling or other roughhousing activities
- Is initiated against the wishes of the child or vulnerable adult, except if such contact may be necessary to prevent injury to the child or vulnerable adult, or to others, e.g. restraining the child or vulnerable adult to prevent harm to themselves or others
- Could otherwise have been expressed through a verbal request

Personnel must report any physical contact initiated by a child or vulnerable adult that is sexual and/or inappropriate, including but not limited to acts of physical aggression, as soon as possible, to a Senior TSA Representative and also in Solv Safety.

See the Incident Management Procedure, to enable the situation to be managed in the interests of the safety of the child or vulnerable adult, the member of personnel and any other participant(s).

Positive guidance

Personnel will make every effort to ensure that all people participating in any mission expression are aware of the acceptable limits of behaviour.

Personnel will encourage children and vulnerable adults to feel safe, be safe and have positive relationships and friendships with their peers.

Personnel will encourage children and vulnerable adults to 'have a say', especially on issues that are important to them, and to participate in all relevant activities.

Personnel will provide children and vulnerable adults with information about their safe participation in TSA activities including access to information about child and vulnerable adult abuse prevention programs.

At times, personnel may be required to use appropriate techniques and behaviour management strategies in response to behaviour, to ensure an effective and positive environment that is safe for the children or vulnerable adults and the personnel participating in the activity. In these circumstances, personnel will:

- Only use techniques they have been trained to use and which are approved as part of the program/activity
- Ensure techniques and behaviour management strategies are fair, respectful and appropriate to the developmental stage of the children and vulnerable adults involved and which uses an appropriate tone of voice
- Ensure the children and vulnerable adults are provided with clear directions and given an opportunity to redirect their behaviour in a positive manner

Under no circumstances are personnel to take disciplinary action against another individual involving physical punishment or any form of treatment that could reasonably be considered as degrading, cruel, frightening or humiliating.

One-on-one interactions

Personnel are required to avoid one-on-one unsupervised interactions with children to whom TSA provides services, and (where possible) to conduct all activities and/or discussions with children in a location that allows them to be visible by other Personnel.

One-on-one interactions with vulnerable adults must not take place unless authorised i.e. funding agreement or practice guidelines.

Any one-on-one interactions in closed, non-visible or private spaces are not considered normal process and must only occur with the full knowledge and written approval of the Senior TSA Representative or as per regulatory guidelines and TSA's processes.

Any one-on-one interactions must comply fully with regulatory and statutory policy and procedural guidelines and requirements of TSA.

Written approval from Senior TSA representatives or parent/guardian must be obtained and recorded prior to any one-on-one interactions as defined.

Social interactions

Personnel must not seek to make or initiate contact or spend time alone with any child or vulnerable adult outside their stated role and responsibilities, including but not limited to personal social media and other web-based networks or forums, face to face and phone contact.

Where contact outside a program is necessary, prior written approval must be obtained and recorded from the parent/guardian and the Senior TSA Representative, and such contact must occur in the presence or sight of another adult.

Where a pre-existing relationship exists with any child regardless of whether they are a current or previous client, personnel must have written permission from the parent/guardian and have disclosed the relationship to the Senior TSA Leader. Failure to make such a declaration is a breach of the Code of Conduct.

See the Conflict of Interest Procedure and Conflict of Interest Disclosure Form

Safeguards in Program and Activities Guidelines

Supervision

Personnel are responsible for supervising children and vulnerable adults, and all other people they are likely to interact with whilst engaged with TSA. In so doing, personnel are required to ensure, to the best of their ability, that the children and vulnerable adults and any other people present:

- Engage positively
- Behave appropriately towards one another, e.g. are respectful of others and do not engage in behaviours that are discriminatory, aggressive, otherwise abusive or illegal
- Are in a safe environment and are protected from external threats

Overnight stays, camps and sleeping arrangements

Overnight stays for any child are to occur only with the written authorisation of the parent/guardian and the written authorisation of the appropriate Senior TSA Representative.

Practices and behaviour by personnel during an overnight stay must be consistent with the practices and behaviour defined in this Code of Conduct Standard as is expected during the delivery of all TSA programs.

Personnel shall never invite or arrange for a child engaged or previously engaged in any capacity with TSA to stay overnight at their home or with them, unless they are the parent or guardian of that child.

Personnel shall never invite a vulnerable adult to stay overnight at their home or with them.

With the exception of family, extended family and friendship groups, trips approved by TSA involving overnight stays will ensure that:

- A documented risk assessment is conducted prior to the event and approved by the appropriate Senior TSA Representative

- All personnel engaged in providing overnight stays and camps will have current police check and WWCC (relevant to state/territory requirements) which has been validated in line with the WWCC regulator requirements, with no issues of concern noted, and has been linked to TSA prior to the event, as required by law.
- Parent/guardian knowledge and consent is provided in writing prior to the event
- All accommodation and sleeping arrangements do not compromise the safety of any child, such as unsupervised sleeping arrangements, mixed gender sleeping arrangements or an adult sleeping in the same room or bed as a child
- All showering and personal care arrangements must be managed and supervised (as appropriate to the age and needs of each child) by personnel balancing the requirements of each child's right to privacy while also ensuring that:
    - Personnel avoid one-on-one situations with any child or vulnerable adult in a change room area
    - Personnel do not use a change room area while children or vulnerable adults are present, for any other reason than to provide appropriate supervision
    - Personnel provide adequate supervision in 'public' change rooms when these spaces are used
    - Personnel provide the level of supervision required to prevent abuse, neglect, harm or risk of harm by members of the public, adult service users, peer service users and general misbehaviour
    - Female personnel do not enter male change rooms, and male personnel do not enter female change rooms (refer to the Gender Affirmation in the Workplace Guidelines for additional guidance for transgender people and non-binary people)
- Personnel are aware of the location of all children and vulnerable adults in their care, at all times
- Children have the right to contact their parent/guardian or any other person they choose, if they feel unsafe, uncomfortable or distressed during the stay

Transportation

The transportation of any child or vulnerable adult will only occur where the following conditions are met.

The transport is:

- Directly related to the mission delivery of TSA
- Explicitly stated in the activity information provided to the parents/guardians
- Recorded as part of the activity risk assessment

Children or vulnerable adults must only be transported where:

- Prior authorisation has been received from the appropriate TSA representative
- The written consent of the parent/ guardian has been received

Gaining authorisation to transport requires the personnel involved to provide information about the proposed journey, including the:

- Type of transport proposed, e.g. private car, taxi, self-drive bus, bus with driver, train, plane, boat, etc.
- Reason for the journey
- Route to be followed, including any stops or side trips
- Details of all persons who will be present during the journey including personnel

Suitable activities

Personnel engagement with children or vulnerable adults should empower the children or vulnerable adults to participate more effectively in TSA.

All actions and interactions by personnel with children or vulnerable adults will consider and respect the strengths and individual characteristics of each child or vulnerable adult regardless of their abilities, cultural background, sexual orientation, gender identity, gender expression, intersex status or social economic background.

Personnel will:

- Engage the parents/guardians and caregivers as the best source of information about how to include children with additional needs in activities
- Demonstrate respect for children and vulnerable adults with additional needs who may require additional help with personal self-care activities
- Encourage and guide children and vulnerable adults to behave and interact with respect, honesty and fairness
- Ensure children and vulnerable adults understand how to raise any concerns and issues they may have, and are aware of who, within TSA, they can raise their concerns with
- Not hire children for domestic or other labour which:
    - Is inappropriate, or illegal given their age or developmental stage
    - Interferes with their time available for education and recreational activities
    - Places them at significant risk of injury

Communication with Children and Vulnerable Adults

Electronic communications

All electronic communication with children and vulnerable adults should be restricted to issues directly associated with the delivery of TSA services.

Wherever possible, a parent/ guardian is to be copied into all email and text messages sent to a child/vulnerable adult. Where this is not possible, another TSA personnel member must be copied into all electronic communications.

In all electronic communications with a child/vulnerable adult, personnel will:

- Limit the content to that required to convey the service-related message in a polite, friendly manner
- Not communicate anything that a reasonable observer could view as being of a sexual nature
- Not promote any unauthorised 'social' activity or attempt to arrange any unauthorised contact
- Not request a child or vulnerable adult keep any communication secret from their parents/guardians
- Not communicate with children or vulnerable adults using Internet chat rooms or similar forums including but not limited to social networking sites, game sites or instant messaging

Technology

Personnel will not use computers, mobile phones, or cameras for the purposes of, or in a manner that could be deemed to be, exploiting or harassing a child or vulnerable adult or that are contrary to TSA policies and procedures.

Images

To ensure the privacy and safeguarding of children and vulnerable adults when photographing, filming or using images or stories for any TSA related activities including promotion, fundraising and development education, personnel will:

- Not photograph or record any children or vulnerable adults without their informed consent and/or the consent of the parent/guardian of children, or where the child or vulnerable adult is in the care of TSA, the applicable Senior TSA Representative
- Not publish or share photographs or recordings of any children or vulnerable adults if there is known to be any kind of Court order in relation to them
- Only photograph or record children or vulnerable adults using TSA devices and not personally owned devices
- Only photograph or record children or vulnerable adults wearing suitable clothing they would be expected to be seen wearing in a public place
- Not photograph children or vulnerable adults with identifying information such as full names, wearing school uniforms or identifying other places the person regularly attends
- Only photograph or record children or vulnerable adults in the presence of another member of personnel
- Take care to assess and comply with local cultural traditions and/or restrictions on taking and reproducing personal images and recordings and in obtaining stories of children or vulnerable adults before photographing or filming

- Provide an explanation of how and where any images and recordings taken, will be used
- Ensure all images and recordings present children and vulnerable adults in a dignified and respectful manner and not in a vulnerable, degrading or submissive manner
- Ensure that children or vulnerable adults are adequately clothed and not in poses that could be viewed as sexually suggestive
- Ensure file labels, metadata and text descriptions do not reveal any identifying information about the child/vulnerable adult when sending or publishing images or stories in any form

The taking and use of images and stories must be in line with TSA's policies and procedures and be in accordance with all relevant regulatory and legislative requirements and funding body guidelines.

Diversity and Safety

Diversity and social inclusion

Personnel will be considerate, respectful and embracing of cultural and family traditions and support structures.

TSA is committed to ensuring it meets its corporate, social, ethical and spiritual obligations for reconciliation through participation and engagement with and alongside Aboriginal and Torres Strait Islander peoples.

Personnel will:

- Ensure programs and activities do not discriminate on the basis of sex and sexual identity, gender and gender identity, colour, race, age, religious beliefs or ability
- Ensure that their approach and interactions with all people are sensitive, respectful and inclusive of all backgrounds and abilities
- Ensure activities are inclusive and flexible enough to meet the needs of all participants
- Ensure the safety (including cultural safety), participation and empowerment of children and vulnerable adults who:
    - Are Aboriginal or Torres Strait Islander
    - Are from culturally and/or linguistically diverse backgrounds
    - Have a disability
    - Have a diverse sexual orientation or gender identity

See the Diversity and Inclusion Policy.

Work health and safety

TSA is committed to delivering its Mission Expressions, including Mission Enterprises, in a manner that balances the interests of all people through a commitment to health and safety.

Personnel are responsible for taking all reasonable steps to prevent workplace injuries and illnesses, to cooperate with management in the best interests of health and safety and to contribute to a safe working environment.

Personnel must not place at risk the health and safety of any person in the workplace.

Bullying and harassment

Personnel must never act in a manner that is discriminatory, bullying or harassing.

Personnel will never humiliate, victimise, intimidate or threaten any person in a direct or indirect manner.

Personnel must not disadvantage someone because of an actual or perceived personal characteristic, such as:

- Age
- Industrial activity
- Parental status
- Political belief
- Personal association
- Race or ethnic background
- Carer status
- Relationship status
- Intersex status
- Gender identity or gender expression
- Sexual orientation
- Pregnancy
- Lawful sexual activity
- Impairment or disability
- Unrelated criminal record
- Religious beliefs or activity
- Physical features

The Code of Conduct for Aged Care

Additional application of the Aged Care Code of Conduct and Banning Orders Register will apply for TSA, an aged care worker of TSA, and a governing person of TSA.

Any person to whom the Aged Care Code of Conduct or Banning Orders Register applies is required to adhere to the conditions contained therein.

Note that the Code does not apply to the Commonwealth Home Support Programme (CHSP) or The National Aboriginal and Torres Strait Islander Flexible Aged Care Program (NATSIFACP).

The NDIS Code of Conduct

Additional application of the NDIS Code of Conduct and Banning Orders Register will apply for TSA and our employees. The application includes members of the key personnel of TSA; unregistered NDIS providers and their employees; NDIS providers delivering information, linkages, and capacity building (ILC) activities; and providers delivering Commonwealth Continuity of Support Programme services for people over the age of 65.

Any person to whom the NDIS Code of Conduct or Banning Orders Register applies is required to adhere to the conditions contained therein.

Use of IT Resources

Use and ownership

TSA provides Information and Communications Technology (ICT) resources to personnel for the purpose of performing their role within TSA. TSA retains ownership of these resources.

Right to monitor and review

TSA reserves the right to monitor and review the use of its ICT resources including notebooks, tablets, desktop computers and mobile phones, and to access all data held on these resources.

This data includes, but is not limited to:

- Internet traffic
- Email messages
- Instant messaging
- Encrypted traffic and information

The use of TSA ICT resources, constitutes user consent to such monitoring and reviewing.

Personal use

Personnel may occasionally use TSA resources, including ICT resources, for limited personal use. Any such use must be pre-approved by the relevant TSA personnel, appropriate and kept to a minimum.

Personal business or activities

TSA resources must not be used to support secondary employment, outside business ventures or personal political activities.

Inappropriate use

Personnel must not use TSA ICT resources in an inappropriate manner. Inappropriate use includes, but is not limited to:

- Engaging in illegal or unlawful activity
- Viewing inappropriate material, including adult or pornographic sites, hate sites, gambling sites or sites which would put TSA's brand and reputation at risk
- Downloading and installing unauthorised applications
- Installing any copyrighted software for which TSA does not have an active licence
- Deliberately introducing malicious programs onto the network (e.g. viruses, worms, Trojans, etc.)
- Accessing data or systems in an unauthorised way
- Using client/participant data to gain access to the client/participant
- Creating a network disruption by conducting activities without authorisation (i.e. network sniffing, packet spoofing and other actions that maliciously attack information)
- Providing information about TSA personnel to external parties without appropriate consent
- Gaining unauthorised access to websites or databases and altering their content
- Excessive use of the Internet, including but not limited to downloading of movies, YouTube, etc
- Use of peer-to-peer software and unauthorised cloud storage
- Removal of assets without prior approval
- Tampering with ICT resources
- Connect unauthorised devices to the network without the appropriate prior approval

Defamation

Personnel must not use TSA ICT resources to send material that defames an individual, organisation, association, company or business. The consequences of a defamatory comment may be severe and give rise to personal and/or TSA liability.

Information Sharing

TSA personnel must not share information of a confidential or sensitive nature to external parties without authorisation from their manager or the information asset owner.

Copyright infringement

Copyright material of third parties must not be used without authorisation. This includes software, database files, documentation, cartoons, articles, graphic files, music files, video files, books, text and downloaded information.

The ability to forward, distribute and share electronic messages, attachments and files greatly increases the risk of copyright infringement. Copying material to electronic storage, or printing, distributing or sharing copyright material by electronic means may give rise to personal and/or TSA liability, despite the belief that the use of such material was permitted.

Information Backup

TSA information

TSA information must be stored in authorised repositories (e.g. file servers or applications). Personnel should not store TSA information in removable media or computers or other devices that are not subject to TSA information backups.

Personal information

Personnel are accountable and responsible for backing up any personal information stored on removable media or computers or other devices.

IT Asset Security

Cybersecurity

Personnel have an obligation to keep TSA ICT resources safe from viruses, malicious software programs and intrusion attempts.

Personnel must not:

- Physically tamper with any TSA issued ICT resources
- Disable or modify the configuration of the security software installed on any TSA ICT resource
- Modify the configuration of the operating system installed on any TSA ICT resource

Cybersecurity incident

Personnel must immediately report any suspected cybersecurity incident to TSA's Information Technology Services (ITS) Service Desk.

Unattended ICT resources

ICT resources must be secured or locked away when unattended to avoid theft. This includes locking the computer screen when the computer is unattended.

User Accounts and Authentication Credentials

Responsibility

Personnel are accountable and responsible for all activity performed with their individually-assigned user account (or user ID) and/or with their TSA ICT resources.

Personal use

Personnel must not use any issued user account (or user ID) or password for personal use or to access any non-TSA online services (e.g. Facebook, LinkedIn, eBay, Gmail, Hotmail, or a personal banking account).

Sharing of passwords

Personnel must not share or disclose their password. Passwords should be protected while they are being typed in to prevent shoulder surfing.

Password storage

Personnel must not write down authentication credentials on paper or in electronic documents (e.g. text files, Word and Excel documents). If required due to business needs, a secure password software solution must be installed by contacting ITS Service Desk.

Remote Access

Personnel must use Multi Factor Authentication (MFA) if available, when accessing TSA systems or information via the Internet.

Breach/ disclosure

Personnel must immediately report any password breach or disclosure to the ITS Service Desk.

Removable Media

Use

The use of removable media storage devices increases the likelihood of information loss and unauthorised disclosure, which could place TSA's brand and reputation at risk.

Sensitive or confidential information must not be stored in removable media storage devices unless the media device is encrypted.

The ITS Department will assist with encrypting removable media storage devices.

Security responsibility

Personnel are accountable and responsible for the security of the information they store in removable media storage devices and must comply with all applicable policies, procedures and regulatory requirements relating to information security.

Hardware

Only ITS approved removable media storage hardware can be used to store sensitive and confidential TSA information.

Personal removable media storage devices must never be used within TSA's ICT environment.

Use of Personal Devices

Use of Personal Mobile Devices

Personnel who wish to use a personal device to store and/or access TSA's information, must first have approval from the appropriate Senior TSA Representative. A personal device used for work purposes may be referred to as a Bring Your Own Device (BYOD).

Personal mobile telephone

Personnel who wish to use their personal mobile telephone to store and/or access TSA's information, must allow TSA to install security software in order to protect TSA's information stored in the device.

Monitor and review

TSA reserves the right to monitor and review the use of any device used to store and/or access TSA's information.

Monitoring and reviewing includes tracking the location of the phone in case it is lost. The use of any device by personnel, to store and/or access TSA's information constitutes consent of the user to such monitoring and reviewing.

Personal information

Personnel are accountable and responsible for the security and backup of any personal information saved on a BYOD.

BYOD data wipe

TSA reserves the right to wipe/erase, via remote access or otherwise, any TSA information (e.g. emails) stored on a BYOD.

Notebooks and Mobile Devices Used to Store and/or Access TSA Information

Security software

Personnel must not disable any security software installed by TSA on these devices.

Application updates

Available software updates should be installed on these devices as soon as they are available.

Jailbreak/ rooting

Personnel must not jailbreak or root any such devices.

Applications must only be installed from trusted sources (e.g. business catalogue or Android Play/ Apple Store).

MMS, SMS and IM

Personnel must not use Multimedia Message Service (MMS), Short Message Service (SMS) or Instant Messaging (IM) to communicate TSA information that is sensitive or confidential.

Device wipe and collection

TSA reserves the right to wipe/erase, via remote access or otherwise, any TSA issued device, and collect any such devices (1) upon termination of employment or service arrangement with TSA; and (2) at any time and without notice.

Personal information

Personnel must not save personal information to any TSA ICT resource.

Commuting and Travelling

Commuting and traveling

The nature of portable devices, such as notebooks, laptops and mobile phones, makes them a target for professional thieves.

When travelling with portable devices, personnel must always retain control over these devices. This includes:

- Never leaving them unattended

Personnel are accountable and responsible for the physical security of any TSA issued device as well as any personal device used to store and/or access TSA information.

Customs inspections

If personnel are requested to decrypt a portable device or any media for inspection by customs officials, or they lose possession of their device at any time, they must report the potential compromise of information to the ITS Service Desk as soon as possible.

E-mail Communications

Mass distribution and SPAM

Personnel must not use TSA email services for sending 'junk mail', for any for-profit messages or chain letters. Mass electronic communications should only be sent in accordance with TSA internal policies and procedures.

Forwarding

Users may not setup 'auto-forwarding' of emails from their TSA email account to any external email account without prior formal approval from the ITS department. This approval should be sought via the ITS Service Desk.

Confidentiality and privacy

Email is not a secure means of communication, particularly when used to communicate to external parties.

Personnel must not use email to send sensitive or confidential TSA information to recipients outside TSA unless the email is encrypted.

The ITS Department will provide advice on secure transmission of information to recipients outside TSA.

Use of Artificial Intelligence (AI) Systems

Approach

TSA recognises the benefits that the use of AI systems can bring. They have the potential to automate tasks, improve decision-making and provide valuable insights, thus increasing the productivity of TSA and its personnel.

However, the use of AI tools presents new challenges in terms of information security, confidentiality, data protection and our relationship with clients and other external stakeholders. This section provides safeguards to ensure responsible and ethical use of AI systems to protect the rights and interests of individuals, maintain legal compliance and uphold TSA's reputation.

All personnel must promptly report any suspected misuse of AI systems to the IT Service Desk or their Senior TSA Representative.

The use of AI systems also increases the likelihood of cyberattacks. For more information on obligations in relation to cybersecurity, please refer to IT Asset Security.

Responsible and ethical use

AI systems should be used in a manner that aligns with TSA standards of behaviour as outlined in this standard. Personnel are prohibited from using AI systems to create content that is illegal, discriminatory, defamatory, or otherwise offensive or inappropriate.

AI systems, particularly generative AI tools, may perpetuate and reflect existing biases contained in the data which is input into them for use and for training. This may have a discriminatory, unfair or unreasonable impact on particular individuals or groups of people.

In using AI systems, personnel must take care to test and rectify any potential or actual bias or discrimination based on an individual's cultural background, age, disability, religious belief, family status, gender identity or expression, intersex status, sexual orientation, or social or economic background.

Privacy and data protection

The use of AI systems must comply with applicable laws and regulations, including but not limited to, the Privacy Act 1988(Cth). If there is a conflict between this standard and any applicable laws and regulations, the laws and regulations will prevail.

It is important to note that data entered into an AI system should be treated as an external disclosure and subject to TSA's policies regarding data confidentiality and security. This is because, for instance, when a question or prompt is entered into an AI system (including but not limited to a generative AI tool), it is possible that any sensitive or confidential information provided could be added to the tool's wider data model and made accessible to others in a future request.

Accordingly, personnel must not upload or share any data that is confidential, proprietary or protected by regulation without relevant prior approvals. Likewise, personal or sensitive information must not be used when interacting with AI systems, unless prior informed consent has been obtained from the individual concerned, and any such use must be in line with TSA's Knowledge, Information and Data Management Policy.

Human oversight and transparency

AI-generated outputs are susceptible to errors, inaccuracies, and inefficiencies. Further, AI systems may generate false or misleading data, which may result in serious consequences particularly where such data is used in communications or for decision making. As such, personnel should not rely solely on content generated by AI systems or make important decisions based on AI-generated outputs alone. Instead, personnel must ensure that any content generated by AI systems is properly reviewed before it is communicated or used for decision-making to ensure accuracy and appropriateness. It is critical that the responsible individual carefully reviews all AI-generated information. Responsibility for any actions, decisions or communications made in connection with that information, including any harm it may cause, resides with the individual who has generated the content Any false or misleading information contained in AI-generated content should be rectified before it is used or distributed.

Awareness and training

It is the responsibility of all personnel to familiarise themselves with TSA's AI-related policies, including any policy updates in response to changes in this rapidly developing area of technology. From time to time, TSA may hold training programs to educate personnel on AI-related issues.

The Salvation Army Image

Use of brand

TSA is a well-recognised movement, respected by many, with an easily identifiable brand.

TSA's logo, images, videos and brand guidelines are only to be used for official activities of TSA and are not for private or personal use.

Personnel shall ensure their use of TSA's logo and brand assets complies with the Brand Policy and guidelines.

Public comment

Unless authorised in accordance with TSA's Media Relations Policy, personnel must not make any public comment on behalf of TSA or make any comment that could be misinterpreted as the view of TSA.

Personal use of social media

Personnel:

- Are required to exercise professional judgement in their use of social media and other personal online activities
- Must not post any content that may damage the reputation of TSA, another organisation or any individual. This also pertains to the disclosure of current and/or ongoing personnel, policy and operational matters or confidential and sensitive information, as it relates to TSA, or with others
- Any requests for comment from media must be directed to the Media Relations department: mediarelations@salvationarmy.org.au
- Must not post any content that includes representation of children or vulnerable adults, without written permission from the child or vulnerable adults' parent/ guardian. Verbal consent from the child or vulnerable adult must also be sought
- Personal views are not to be presented as the position of TSA and must be clearly identified and stated as a personal view, written within the post or message. Content must not contradict TSA's Mission or Values. Failure to comply may result in disciplinary action

Alcohol, smoking and non-medical prescribed drugs

The use of alcohol or any other substance must not adversely affect your work performance or the health and safety of others in the workplace.

Personnel must not consume alcohol while on duty in their respective capacity with TSA, or during any meal breaks.

Personnel must not smoke, including vaping, while wearing TSA branded clothing, while representing TSA in any capacity, while in any TSA building or vehicle or while in the vicinity of any entrance to a TSA building.

Personnel must not supply, receive or use alcohol or any other type of drug (legal or illegal) with any service recipient, irrespective of the service recipient's age.

Personnel are prohibited from the manufacturing, distributing and/or use of any controlled substance in the workplace, or while conducting business on behalf of TSA or while in partnership with TSA.

TSA recognises the need to respond sensitively to the needs of vulnerable groups, and that exceptions to these rules may occur from time to time with prior approval and authorisation of an appropriate Senior TSA Representative.

Gambling

Gambling is contrary to the ethos of TSA. Raffles, sweeps and all other activities associated with gambling are not permitted on TSA's premises.

Personnel are not permitted to engage in any activity associated with gambling while representing TSA.

Political affiliations and contributions

TSA maintains a position of political impartiality.

Personnel must take reasonable steps to ensure that:

- Their political affiliation does not directly or indirectly use TSA funds, resources or assets
- TSA is not associated with any contributions or donations or attendance at political fundraisers

Community Expectations and Values

Human rights and fair trade

Australia is a signatory to the United Nations Declaration on Human Rights.

TSA recognises the inherent dignity of all people and its responsibility to treat them in a fair and equitable manner thereby reflecting TSA's responsiveness to human need.

Modern slavery

In accordance with Modern Slavery legislation, contractors engaged by TSA will certify (and evidence) to the best of their knowledge the products and/or services supplied are ethically sourced.

TSA reserves the right to carry out a due diligence audit if it has any concerns in relation to the Suppliers compliance with Modern Slavery legislation.

Preventing Sexual Exploitation, Abuse and Harassment

Sexual exploitation, abuse and harassment (SEAH) are never acceptable and are not tolerated by TSA. Zero tolerance also applies to inaction in reporting and preventing SEAH.

See the Preventing Sexual Exploitation Abuse and Harassment Standard.

Environment and sustainability

Personnel will strive to meet the highest environmental standards as stated in TSA's Environmental Sustainability Policy.

Stewardship

Personnel will conduct all activities in a responsible manner, consistent with ethical obligations of stewardship and in accordance with all applicable laws, policies and procedures.

Compliance Obligations

TSA Policies

Compliance with The Salvation Army's policies

Personnel will comply with all TSA approved minutes, codes, policies, procedures, standards and guidelines as appropriate, and any reasonable directions by TSA.

Approved authorities

All approvals and financial decisions must be made in accordance with TSA's Approved Authorities Policy and Approved Authorities Matrix.

Gifts and benefits

The receipt of gifts and benefits may be perceived as a conflict of interest. Please refer to the Conflict of Interest Procedure for guidance.

Instances of attempted bribery must be reported to the Internal Audit Department, via the Head of Internal Audit, and in accordance with the Fraud Policy.

Purchasing and supplier management

All supplier selection, management and purchases must be in line with the Procurement Policy and Asset Capitalisation Policy.

Conflict of interest

Personnel must ensure they:

- Disclose any actual, potential or perceived conflict of interest
- Report all conflicts of interest to the appropriate Senior TSA Representative for assessment of the conflict
- Remove themselves from any discussion and/or any decision-making situation where the Chair of a meeting or other Senior TSA Representative has determined the conflict requires that action
- Do not engage in external employment where an appropriate Senior TSA Representative has determined that a conflict of interest exists or may arise, and the conflict is not able to be managed
- Declare any relevant personal relationships when holding a decision-making position, such as supplier selection or purchasing

Details of any actual, potential or perceived conflict of interest are to be reported in writing to the Head of Audit, Risk and Compliance.

Further detail regarding conflicts of interest is available in the Conflict of Interest Procedure.

Secondary employment

Personnel are permitted to work outside/ external to TSA.

Outside/ external work or private work (whether paid or unpaid) must not involve or engage clients (of any age) of TSA in any capacity, with the exception to work that is undertaken through a regulated/ funded program or service or other pre-approved circumstances.

Personnel must not enter into any additional employment which prevents or hinders or is in conflict with TSA.

Procedures relating to outside work are set out in the Secondary Employment Procedure.

Competition

Personnel will not undertake any work that is in competition with TSA or act in a manner contrary to their TSA engagement obligations.

Information technology

Personnel are responsible for managing TSA assets, IT resources, cyber security, physical security, data and access management in accordance with the Information Security Policy.

Knowledge, information and data management

Privacy, intellectual property, record keeping, corporate knowledge, data breach and confidentiality are managed by TSA in accordance with the Knowledge, Information and Data Management Policy.

Theft, fraud and corruption

Any behaviour that is fraudulent, dishonest, corrupt or improper will be managed in accordance with the Fraud Policy.

Whistleblower

All reporting of systemic wrongdoing and/or disclosures of improper conduct within TSA must be addressed in accordance with the Whistleblower Protections Policy.

Legislation

Compliance with laws

Personnel must:

- Follow all applicable laws in all locations where TSA delivers its mission
- Never participate in or assist others to participate in any illegal or criminal activities
- Report any alleged illegal activities or conduct to the relevant authorities and to the applicable Senior TSA Representative

Compliance with integrity checks

Personnel must hold current integrity checks relevant to their role and location, such as a police check and a WWCC, prior to engaging with any child or vulnerable adult. These checks must be renewed prior to expiry and in line with relevant state/territory legislation and the Recruitment and Onboarding Policy and Active Officer Service Conditions and Uniform Policy.

Roles and Responsibilities

The roles associated with execution of this standard are indicated in the table below.

Roles	Responsibilities
Personnel	Personnel are required to perform their duties in accordance with this Standard.
Senior TSA Representative	Supports and advises personnel in relation to the application of this Code of Conduct Standard including: ▪ Ensuring personnel have access to and understand this standard ▪ Ensuring personnel adhere to this Standard

Related Documents and References

Related Policy Documents	Code of Conduct Policy Code of Conduct Standard Conflict of Interest Procedure Conflict of Interest Disclosure Form Gifts and Benefits Disclosure Form Active Officer Service Conditions and Uniform Policy Approved Authorities Policy Asset Capitalisation Policy Brand Policy Diversity and Inclusion Policy Environmental Sustainability Policy Fraud Policy Incident Management Policy Incident Management Procedure Information Security Policy Information and Data Management Policy Media Relations Policy Preventing Sexual Exploitation Abuse and Harassment Standard Procurement Policy Recruitment and Onboarding Policy Remuneration and Conditions Policy Safety and Wellbeing of Children and Young People Policy Secondary Employment Procedure Whistleblower Protections Policy Work Health and Safety Policy
Related Legislation	*Aged Care Act 1997* *Children and Young People Act 2008* (ACT) *Crimes Act 1900* (ACT) *Ombudsman Act 1989* (ACT) *Working with Vulnerable People (Background Checking) Act 2011* (ACT) *Child Protection (Working with Children) Act 2012* (NSW) *Children and Young Persons (Care and Protection) Act 1998* (NSW) *Children's Guardian Act 2019* (NSW) *Crimes Act 1900* (NSW) *Criminal Records Act 1991* (NSW) *Child Protection (Working With Children) Amendment (Statutory Review) Act 2018* (NSW) *Crimes Act 1900* (NSW) *Care and Protection of Children Act 2007* (NT) *Criminal Code Act 1983* (NT) *Domestic and Family Violence Act 2007* (NT) *Child Protection Act 1999* (Qld) *Criminal Code Act 1899* (Qld) *Criminal Law (Rehabilitation of Offenders) Act 1986* (Qld) *Working with Children (Risk Management and Screening) Act 2000* (Qld)

	Child Safety (Prohibited Persons) Act 2016 (SA) *Child Safety (Prohibited Persons) Regulations 2016* (SA) *Children Young People (Safety) Act 2017* (SA) *Criminal Law Consolidation Act 1935* (SA) *Spent Convictions Act 2009* (SA) *Children, Young Persons and their Families Act 1997* (Tas) *Criminal Code Act 1924* (Tas) *Registration to Work With Vulnerable People Act 2013* (Tas) *Child Wellbeing and Safety Act 2005* (Vic) *Children, Youth and Families Act 2005* (Vic) *Working With Children Act 2005* (Vic) *Wrongs Act 1958* (Vic) *Children and Community Services Act 2004* (WA) *Criminal Code Act Compilation Act 1913* (WA) *Equal Opportunity Act 1984* (WA) *Working with Children (Criminal Record Checking) Act 2004* (WA) *Fair Work Act 2009* (Cth) *Privacy Act 1988* (Cth) *Crimes Act 1914* (Cth) *Criminal Code 1995* (Cth) *Disability Discrimination Act 1992* (Cth) *Evidence Act 1995* (Cth) *Racial Discrimination Act 1975* (Cth) *Sex Discrimination Act 1984* (Cth)
Other Relevant Documents /Resources	Definition of Intersectionality adapted from *'Understanding intersectionality' Victoria State Government website*. *Code of Conduct for Aged Care – Guidance for providers* *NDIS Code of Conduct for providers, their employees and members of Key Personnel* *Code of Conduct for Aged Care (the Code)* *Approved Provider* *An aged care worker of an approved provider* *A governing person of an approved provider* *Key Personnel* *Aged Care Register of Banning Orders* *NDIS Code of Conduct* *NDIS Code of Conduct for Workers* *NDIS Banning Order Register*

Definitions

Definitions are located in the Glossary of Terms and Definitions.

Term	Definition
Boundaries	Boundaries are guidelines, rules or limits that create reasonable, safe and permissible ways for people to engage and behave with others, both personally and professionally. **Physical boundaries** Physical boundaries refer to personal space and physical touch. Healthy physical boundaries include an awareness of what is appropriate and what is not appropriate in various types of settings and relationships. **Psychological and emotional boundaries** Psychological and emotional boundaries refer to a person's feelings. Emotional boundaries may be violated when someone criticises, belittles or invalidates another person's feelings. Healthy emotional boundaries include limitations on when to share or when not share personal information. **Sexual boundaries** Sexual boundaries refer to the emotions, intellectual and physical aspects of sexuality. Sexual boundaries may be violated with unwanted sexual touch, pressure to engage in sexual acts, or sexual comments. Healthy sexual boundaries involve mutual understanding and respect of limitations between people. **Professional boundaries** Professional boundaries are the legal, ethical and organisational frameworks that protect clients/ participants/ beneficiaries from physical and emotional harm and help maintain a safe environment. These boundaries can be challenging in situations including where a client/ participant/ beneficiary: ▪ Offers personnel a gift ▪ Invites personnel to a social function or their home ▪ Wants to extend the relationship beyond program/ service/ activity in which they are engaged e.g. becoming friends ▪ Divulges personal information beyond the scope of the professional relationship (Relationships Australia)
Cyber-Attack	An attack via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.
Cybersecurity Incident	An event that actually or potentially jeopardises the: ▪ Confidentiality, privacy, integrity, or availability of an information system ▪ Actual information that the system processes, stores, or transmits or an event that constitutes a violation or imminent threat of violation of TSA's Code of Conduct Policy or Information Security Policy and/or their associated procedures.
Gender Expression	The ways in which a person expresses their gender identity. This can include appearance, behaviour and mannerisms such as how someone dresses, wears their hair, if they use make-up, their body language and their tone of voice. A person's name and pronouns are also common ways of expressing gender, and this is the case for transgender people as well as cisgender people.
Gender Identity	Refers to a person's internal, deeply felt sense of being either man, woman, non-binary, or a range of other gender identities. Because gender identity is internal and personally defined, it is not always visible to others and therefore should not be assumed.

Term	Definition
Grooming	Any behaviour regarded as "grooming" either of a child, or of an adult with the purpose of gaining access to that individual, sexual contact and/or exploitation is unacceptable, including but not limited to: ▪ Developing a "special" relationship by spending inappropriate "special time" with them, giving gifts, showing favours, allowing the individual to overstep boundaries and rules or asking the child to keep the relationship secret ▪ Testing boundaries with an individual by encouraging inappropriate physical contact including "accidental" intimate touching, talking about sex or sexual behaviours ▪ Inappropriate personal communications, including emails, text messaging, social media and web-based contact, that seeks to establish a relationship ▪ Extending a relationship with a child outside personnel stated role and responsibilities ▪ Requesting a child to keep any aspect of the behaviour, actions or communications of a member of personnel secret Grooming can also occur online. When a child is groomed online, groomers may hide who they are by sending photos or videos of other people, often representing themselves as someone younger to gain trust. Like direct grooming behaviours, online groomers will use tactics such as giving individual attention to a child, buying gifts, isolating child from friends and family introducing the idea of 'secrets' to control, frighten and intimidate. Online groomers may target one child online or contact lots of children quickly and wait for them to respond. A groomer will use the same sites, games, and apps as young people, spending time learning about a child's interests and using this to build a relationship with them. Children can be groomed online through a range of media channels including: social media, text messages, email, text, voice and video chats.
Harm or Risk of Harm	Includes physical harm or psychological harm (whether caused by an act or omission) and includes harm caused by sexual, physical, emotional abuse, exploitation, and neglect.
Information and Communications Technology (ICT) Resource	Resources including desktop computers, notebooks, mobile phones, tablets, Internet access, email services, networks, applications and storage.
Information Asset Owner	The role with operational authority for specified information asset and responsibility for establishing controls for its protection.
Intersex	People born with physical sex characteristics that don't wholly or solely fit into the binary medical definitions of male or female. This includes naturally occurring and very normal differences of chromosomes, gonads (ovaries and testes), hormones, and/or genitals. There are more than 40 intersex variations.
Jailbreak/Rooting	The modification of a smartphone or other electronic device to remove restrictions imposed by the manufacturer or operator to allow installation of unauthorised software.
Operating System	A program that runs on a computer and provides a software platform on which other programs can run, e.g. Microsoft Windows 10.
Passphrase	A memorised secret phrase consisting of a sequence of words or other text that a claimant uses to authenticate their identity. A passphrase is similar to a password in usage but is generally longer for added security, e.g. "I love working at TSA because we help people!"

Term	Definition
Password	A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorisation.
Security Software	Software deployed in ICT resources to protect them from cyber-attacks and unauthorised disclosure of information e.g. antivirus, mobile device management, data loss prevention, end-point compliance and data encryption.
Sexual Orientation	Sexual orientation refers to a person's sexual and relationship preferences as it relates to gender. For example, whether they are attracted to people of the same or opposite sex, to both men and women or to people who are non-binary. Others may describe themselves as not experiencing sexual or romantic attraction.
Sexual Misconduct	Sexual misconduct encompasses a range of actions that would reasonably be considered to be sexual in nature, including but not limited to: ▪ 'Contact behaviour', such as sexual intercourse, kissing, fondling, sexual penetration or exploiting a person through prostitution ▪ 'Non-contact behaviour', such as flirting, sexual innuendo, inappropriate text messaging, inappropriate photography or exposure to pornography or nudity
Shoulder Surfing	The practice of spying on a user of an ATM, computer, or other electronic device in order to obtain their authentication credentials.
User Account, User ID, Login ID	A unique symbol or character string used by an information system to identify a specific user.

Document Control Information

Theme	Governance
Category	Legal, Risk and Compliance
Policy Owner	Chief Secretary
Policy Implementer	Secretary for Personnel
Approval Authority	Australia Territory Board
Review Date	August 2023
Next Review Date	October 2026

Document History

Date	Summary of Changes
08/08/2019	Inaugural version
12/03/2021	12 month review
29/03/2021	Amendment to requirements for overnight stays
1/12/2021	Policy Owner and Implementer update and updated according to Rainbow Tick requirements
04/04/2022	Updated to include harm or risk of harm
13/12/2022	Updated to include references to Aged Care and NDIS Codes of Conduct.
29/05/2023	Updated Personal use of social media section
28/08/2023	Updated Relationships with clients/participants section, WWWC section, Boundaries and Social Interactions section.
19/10/2023	Added section related to use of AI
10/05/2024	Updated the reference to the NDIS Code of Conduct
16/04/2025	Added sections related to the Code of Conduct for Aged Care and NDIS Code of Conduct for Providers; added detail related to wearing TSA branded clothing; added reference to Secondary Work Procedure