Code of Conduct Standard

Contents

Overview

Purpose	This document defines the expected standards of behaviour, conduct, and responsibilities for personal conduct when engaging with TSA.
Who does this apply to?	This procedure applies to: ▪ All personnel of The Salvation Army (TSA) Australia Territory ▪ Anyone who engages with TSA
Effective date	06/09/2019

Definitions

Term	Definition
Abuse	Abuse refers to all forms of: ▪ Physical abuse ▪ Emotional abuse ▪ Spiritual abuse ▪ Sexual abuse and exploitation ▪ Grooming behaviours ▪ Neglect or negligent treatment ▪ Commercial (e.g. for financial gains) or other exploitation of a person ▪ Actions that result in actual or potential harm or injury to a person Abuse can be a single incident, but usually takes place over time.
Authentication credentials	Any form of authentication used to validate the identity of an individual. Common authentication information are: passwords, passphrase, private keys, tickets, tokens, etc.
Board, The	The Salvation Army Australia (Territory) Board provides governance oversight to the Australia Territory and has been established to strategically position the Territory so it has a sustainable, major influence on Australian society. The Board provides advice and assistance to the Trustees.
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.
Child, Young Person	Refers to and includes all persons under the age of 18 years.
Conflict of Interest	**Actual conflict of interest** A conflict between the duties and personal interests of an individual that improperly influences the performance of their duties. Apparent or perceived conflict of interest A situation where it appears that an individual's personal interests could improperly influence the performance of their duties but this is not in fact the case.

Term	Definition
Cultural Safety and Inclusiveness	Cultural safety refers to "an environment that is safe for people: where there is no assault, challenge or denial of their identity, of who they are and what they need. It is about shared respect, shared meaning, shared knowledge and experience, of learning, living and working together with dignity and truly listening." Williams, R. (2008) Cultural safety; what does it mean for our work practice? *Australian and New Zealand Journal of Public Health*, *23(2),* 213-214. Cultural safety also refers to creating an environment that: ▪ Empowers individuals to actively participate in activities believing they are valued, understood and taken seriously ▪ Supports individuals to carry out culturally significant tasks as part of their involvement in activities or programs run by or on behalf of The Salvation Army
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 occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Discrimination	Disadvantaging someone because of an actual or perceived personal characteristic (protected attribute) as defined in relevant legislation such as: ▪ Age ▪ Physical features ▪ Industrial activity ▪ Parental status ▪ Political belief ▪ Personal association ▪ Race/ethnic background ▪ Carer status ▪ Relationship status ▪ Gender, Gender identity, sexual orientation ▪ Pregnancy ▪ Lawful sexual activity ▪ Impairment/disability ▪ Unrelated criminal record ▪ Religious belief/activity Discrimination occurs if a person treats or proposes to treat a person with a protected attribute less favourably because of that attribute.
Electronic communications	For the purposes of this policy, it refers to emails, instant messaging (e.g. Skype for business), Multimedia Message Service (MMS) and Short Message Service (SMS).
Engaged	Any individual or entity with a formal or informal relationship with The Salvation Army including but not limited to suppliers, service recipients and members of the community.

Term	Definition
Equity and Diversity	Equity ensures everybody has an equal opportunity and is not treated differently or discriminated against because of their characteristics. Diversity takes into account the differences between people and respects the diversity of perspective and contribution of all people. TSA values the diverse skills and perspectives people bring to its operations, mission expressions, and the workplace through their gender, gender identity, age, language, ethnicity, cultural background, disability, religious belief, sexual orientation and marital status.
ICT resource	Any desktops, notebooks, mobile phones, tablets, Internet access, email services, networks, applications and storage amongst others.
Illegal or unlawful use	Illegal or unlawful use includes but is not limited to: ▪ Use of certain types of pornography under Federal or State legislation, such as child pornography ▪ Offences under Federal or State legislation. ▪ Defamatory material ▪ Material that could constitute racial or religious vilification, or unlawfully discriminatory material ▪ Stalking ▪ Harassment ▪ Blackmail and threats ▪ Use that breaches copyright laws, fraudulent activity, computer crimes and other computer offences under Federal or State legislation ▪ Breaches under any other relevant legislation
ICT	Information and communications technology.
Information asset	Any information and underlying supporting infrastructure such as business processes, hardware, networks, applications, third party suppliers and storage amongst others.
Information asset owner	Individual with operational authority for specified information asset and responsibility for establishing controls for its protection.
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.
Mission Expressions	Ministries or services of The Salvation Army that provide holistic mission and serve people in local communities. This includes Corps, Social and Community programs, Chaplaincy and Mission Enterprises. Examples include but are not limited to Corps meetings and programs, accommodation services, Doorways and Salvo Stores.
Mobile devices	Notebooks, mobile phones, smartphones, portable electronic devices, personal digital assistants, tablets and other portable Internet–connected devices.
Operating system	A program that runs on a computer and provides a software platform on which other programs can run. For example, Windows 10.
Passphrase	A passphrase is a memorised secret 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. An example of a passphrase is “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.
Personal information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable: ▪ Whether the information or opinion is true or not ▪ Whether the information or opinion is recorded in a material form or not
Personnel, TSA	A person who may be an officer, territorial envoy, aux-lieutenant, cadet, candidate, person serving under officer conditions, employee, volunteer, a contractor or subcontractor, employee of a contractor or subcontractor, employee of a labour hire company, trainee or student on placement that is engaged in TSA mission delivery or expression, or is a Board or Board Committee member.
Policy owner	The Policy Owner is the delegate to ensure that all policies, procedures and supporting documents are developed, amended, rescinded and reviewed according to the Policy Management Policy (GO_LR_POL_TPMP) and the Policy Lifecycle Procedure (GO_LR_PRO_TPMP). The Policy Owner is responsible for managing the following four stages of the Policy Lifecycle: 1. Identify and Plan 2. Develop, Consult and Approve 3. Implement 4. Monitor and Review
Removable media	Removable media is defined as a storage media that can be easily removed from a system and is designed for removal, for example USB flash drives, DVDs, CDs, portable hard drives and tape-drives.
Security software	Software deployed in ICT resources to protect them from cyber-attacks and unauthorised disclosure of information. Examples of security software are antivirus, mobile device management, data loss prevention, end-point compliance, and data encryption amongst others.
Senior TSA representative	A Senior Manager or above in your direct line of management authority or equivalent.
Sensitive personal information	The following are all types of personal information: ▪ 'sensitive information' (includes 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 (subject to exemptions) ▪ 'tax file number information'
Shoulder surfing	The practice of spying on a user of an ATM, computer, or other electronic device in order to obtain their authentication credentials.
The Salvation Army (TSA)	The Salvation Army in Australia inclusive of all mission expressions.
User account, user ID, login ID	A unique symbol or character string used by an information system to identify a specific user.

Term	Definition
Vulnerable person	Vulnerable Person for the purpose of this standard means: ▪ A child or young person under 18 years of age, or ▪ An individual aged 18 years and above who is or may be unable to take care of themselves, or is unable to protect themselves against harm or exploitation by reason of age, illness, trauma or disability, or any other reason
Working with Children/Working with Vulnerable Persons Checks (WWCC or WVPC)	A Working with Children Check (WWCC) or a Working with Vulnerable Person Check (WVPC) is a specific check required under relevant state/territory legislation for an individual to engage in paid or unpaid child or vulnerable people related activities.

Procedure Statement

Principles

Expectation

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

It is the responsibility of all personnel to read and understand the standards defined in this document.

Equal opportunity

All personnel must never act in a discriminatory way towards others.

See definition of discrimination.

Duty of care

The obligation for care of others must be in accordance with TSA's Duty of Care policy (GO_LR_POL_TDOC).

Behaviours not defined

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

Personal Behaviour

Integrity, honesty and respect

All personnel must conduct themselves with honesty, integrity and transparency at all times.

All personnel will treat others with respect, dignity, fairness and courtesy.

All personnel will treat children and vulnerable people in a manner that conveys their worth as individuals.

All personnel will respect the opinions and beliefs of others and their right to practice their beliefs.

All personnel will demonstrate professionalism and courtesy in dealing with other employees, officers, suppliers, volunteers, contractors, clients, visitors and members of the public.

Dress and appearance

Dress in a neat, clean and appropriate manner for the particular area in which you work.

Includes:	Does not include:
▪ Trousers, business shorts, pants, skirts, dress ▪ 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

Approved variations to the dress code can be defined by program or location Senior Salvation Army Representatives to allow for appropriate community engagement.

Variations to this dress code that may be required based on individual circumstance are to be approved by the site's Senior Salvation Army Representative.

TSA uniform

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

Personal best	Perform your defined duties to the best of your ability. Maintain the expected standard of conduct and work performance.
Sensitive language	All 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: ▪ Background ▪ Family status ▪ Gender or gender identity ▪ Sex or sexual identity ▪ Social, economic or cultural background
Attendance and punctuality	Be punctual and regular in attendance and promptly notify your line manager of any unplanned absence.

Unacceptable Behaviour

The following behaviours are not condoned by TSA for any personnel towards any child, vulnerable person or other individual.

Violence and assault	All personnel must not behave in any way that may be considered violent, aggressive or may constitute assault in any form or manifestation against any person.
Language and verbal abuse	All personnel must not use language that is: ▪ Abusive, uncivil, insulting or obscene ▪ Intended to harm, abuse, bully, harass, shame, humiliate, belittle or degrade ▪ Inappropriate, offensive or discriminatory
Boundaries	Personnel should not, of their own volition or at the request of a child or vulnerable person, act outside the confines of their 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 and sexual boundary limits.
Act and report concern	All personnel must report all concerns, complaints and allegations, and actual or perceived breaches of TSA's policies relating to the safety and wellbeing of any individual to a Senior Salvation Army representative.
Sexual misconduct	Under no circumstances is any form of sexual behaviour to occur between, with or in the presence of children or vulnerable people, irrespective of the age of the child or vulnerable person. 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 Interaction of a sexual or intimate nature is unacceptable with or towards any person, and includes behaviours such as inappropriate touching, flirting, sexual innuendo, conversations (through any medium), comments about an area of the body, a sexual activity or of a sexual nature, exposure to pornography, exposure sexual activity by others, undressing or watching someone else undress.

Exploitation	All personnel shall not seek the influence of any person to obtain promotion or other advantage. All personnel must not exercise any undue influence (whether physical or psychological) over any person including other staff members and clients for a personal benefit or for the benefit of TSA.

Working with Children Guidelines

Working with children/working with vulnerable person check	All personnel engaged in any direct contact or who work with children must hold a valid Working with Children Check/Working with Vulnerable Person Check in the relevant state or territory in which they work.
Power imbalance	All personnel are required to be aware that children and vulnerable persons often have limited or no power or voice in adult-child/adult relationships. All personnel will ensure their behaviour recognises and minimises the power imbalance inherent in your role and position within TSA and does not take advantage of any other individual.
Reporting obligations	All personnel must ensure the safety of all individuals by taking immediate and appropriate action to remove and/or reduce the risk to a child, including the immediate notification of harm or abuse to a Senior Salvation Army representative. All personnel are expected to make a report immediately (i.e. as soon as possible or before the end of the day) if they: ▪ Become aware of any allegations of child abuse ▪ Have a concern for the safety of a child or young person in our services ▪ Notice any personnel member whose practice or behaviour is contrary to the expectations of behaviour set out in this Code of Conduct All personnel must obtain and follow the direction of their line manager or Senior Salvation Army Representative, and in accordance with TSA's Incident Management (GO_QA_POL_TCIM) processes.
Physical contact	Any physical contact with children must be appropriate to the delivery of services and based on the needs of the child (such as to assist or comfort a distressed child) rather than on the needs of our personnel. Under no circumstances should any personnel have contact with children that: ▪ Involves touching of genitals, buttocks or breast area (female children), other than for the purposes of delivering medical or allied health services ▪ Is intended to cause pain or distress to a child, for example, corporal punishment ▪ Is overly physical, includes but is not limited to wrestling, horseplay, tickling or other roughhousing activities ▪ Is initiated against the wishes of the child, except if such contact may be necessary to prevent injury to the child or to others, for example restraining the child to prevent harm to themselves or others Personnel must report any physical contact initiated by a child that is sexual and/or inappropriate, including but not limited to acts of physical aggression, as soon as possible to a Senior Salvation Army Representative, to enable the situation to be managed in the interests of the safety of the child, our personnel and any other participants.

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
Positive guidance	Ensure that children participating in TSA Mission Expressions are aware of the acceptable limits of their behaviour. Children are encouraged to feel safe, be safe and have positive relationships and friendships with their peers. Wherever possible, children are encouraged to 'have a say' and participate in all relevant organisational activities, especially on issues that are important to them. Children are provided with information about their safe participation in organisational activities including access to information about child abuse prevention programs. In circumstances where personnel may be required to use appropriate techniques and behaviour management strategies to ensure an effective and positive environment and/or the safety and/or wellbeing of children or personnel participating in Salvation Army activities, personnel will: ▪ Ensure techniques and behaviour management strategies are fair, respectful and appropriate to the developmental stage of the children involved ▪ The child is provided with clear directions and given an opportunity to redirect their misbehaviour in a positive manner Under no circumstances are personnel to take disciplinary action involving physical punishment or any form of treatment that could reasonably be considered as degrading, cruel, frightening or humiliating.
One-on-one interactions	All personnel are required to avoid one-to-one unsupervised situations with children to whom we provide services, and (where possible) to conduct all activities and/or discussions with service recipients in view of other personnel. Any one-on-one interactions or communications 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 Salvation Army Representative or as per regulatory guidelines and The Salvation Army's processes. Such activities requiring one-on-one interaction must comply fully with regulatory and statutory policy and procedural guidelines and requirements of TSA. Written approval from Senior Salvation Army representatives or parent/guardian must be obtained and recorded prior to any one-on-one interactions as defined.
Social interactions	All personnel must not seek to make or initiate contact or spend time alone with any child or vulnerable persons 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 Senior Salvation Army Representative, and such contact must occur in the presence or sight of another adult.

Children's Program and Activities Guidelines

Supervision

Personnel are responsible for supervising the children engaged with TSA to ensure participants:

- Engage positively
- Behave appropriately toward one another, for example, are respectful of other children and personnel, do not engage in behaviours that are discriminatory, aggressive
- Are in a safe environment and are protected from external threats

Overnight stays, camps and sleeping arrangements

Overnight stays are to occur only with the authorisation of a Senior Salvation Army Representative and the parents/guardians of the children or young people involved.

Practices and behaviour by personnel during an overnight stay must be consistent with the practices and behaviour defined in this Standard and as expected during delivery of TSA programs at other times.

All personnel shall never invite or arrange for a child or vulnerable persons 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.

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 Senior Salvation Army Representative
- All leaders and adults over the age of 18 years have had a police check and WWCC/WVPC undertaken prior to the event
- Parental or guardian knowledge and consent is provided in writing
- All accommodation and sleeping arrangements do not compromise the safety of children, such as unsupervised sleeping arrangements, mixed gender sleeping arrangements or an adult sleeping in the same bed as a child
- All showering and personal care arrangements must be managed and supervised (as appropriate to the age and needs of the child) by personnel, balancing the requirements of a child's right to privacy but ensuring that:
    - Personnel will avoid one-on-one situations with a child in a change room area
    - Personnel are not permitted to use the change room area to, for example, undress, while children are present
    - Personnel will ensure adequate supervision in 'public' change rooms when they are used
    - Personnel will provide the level of supervision required for preventing abuse by members of the public, adult service users, peer service users, or general misbehaviour, while also respecting a child's privacy
    - Female personnel are not to enter male change rooms, and male personnel are not to enter female change rooms
- All personnel must be aware of the location of children at all times
- Children have the right to contact their parents, or others, if they feel unsafe, uncomfortable or distressed during the stay

Transporting children

Children and young people are only to be transported where the following conditions are met.

Transport is:

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

Children must only be transported where:

- Prior authorisation has been received from a designated staff member
- The written consent of the child's parent/guardian has been received

Gaining authorisation involves providing information about the proposed journey, including the:

- Form of transport proposed, including but not limited to private car, taxi, self-drive bus, bus with driver, train, plane, boat
- Reason for the journey
- Route to be followed, including any stops or side trips
- Details of anyone who will be present during the journey other than TSA personnel who are involved in the mission expression activity

Suitable activities

Engagement with children should empower them to participate more effectively in TSA.

All actions and interactions with children will consider and respect the strengths and individual characteristics of children and vulnerable persons regardless of their abilities, sex and sexual identity, gender and gender identity, or social, economic or cultural background.

All personnel will:

- Engage parents and caregivers as the best source of information about how to include children with special needs in activities
- Demonstrate respect for participants with special needs who may require additional help with personal self-care activities
- Encourage and guide children to behave and interact in a respectful, honest and fair way
- Ensure children know how to raise and voice concerns and issues, and are aware of who within TSA they can raise their concerns to

Communication with Children

Electronic communications

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

Wherever possible, email and text messages sent to a child should be copied to their parent or guardian. Where it is not possible for a parent or guardian can be copied in, another adult must be copied into the electronic communication.

Where a parent is not included in the communication, personnel will:

- Limit the personal or social content in such communications to what is required to convey the service-related message in a polite, friendly manner. In particular, personnel will not communicate anything that a reasonable observer could view as being of a sexual nature
- Not use such communication to promote unauthorised 'social' activity or to arrange unauthorised contact
- Not request a child to keep a communication a secret from their parents
- Not communicate with children using Internet chat rooms or similar forums such as social networking sites, game sites or instant messaging

These constraints do not apply to electronic communication with family members.

Technology

Only use computers, mobile phones, or cameras as per TSA's policies and procedures.

Never use computers, mobile phones, or cameras for the purposes of, or in a manner that could be deemed to be exploiting or harassing of a child or contrary to Salvation Army policy.

Images

To ensure the privacy and safeguarding of children and vulnerable persons when photographing or filming or using images or stories for work-related purposes including promotion, fundraising and development education, personnel will:

- Not photograph any children or vulnerable persons without the consent of the parent, guardian, care giver or where in the care of TSA, the applicable Senior Salvation Army Representative
- Only photograph or make any recordings of children in the presence of another member/s of personnel
- Take care to assess and comply with local cultural traditions or restrictions on taking and reproducing personal images or obtaining stories of children and vulnerable persons before photographing or filming
- Provide an explanation of how the images and recordings will be used
- Ensure images (photos, films, videos) present children and vulnerable people in a dignified and respectful manner and not in a vulnerable or submissive manner.
- Ensure that children and others are adequately clothed and not in poses that could be viewed as sexually suggestive
- Ensure file labels, metadata or text descriptions do not reveal identifying information of the child or vulnerable person when sending images electronically or publishing images or stories in any form

The taking and use of images must be in line with TSA's policies, and procedures, as well as in accordance with legislation and funding body guidelines.

Diversity and Safety

Diversity and social inclusion

TSA values the diverse skills and perspectives that all people bring to society and the workplace through their gender, gender identity, age, language, ethnicity, cultural background, disability, religious belief, sexual orientation, working style, educational level, professional skills, work and life experiences, job function, socio-economic background, geographical location, marital status and family responsibilities.

All personnel will be considerate of, respect and embrace cultural and family traditions and support structures.

All 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 children and vulnerable people are sensitive, respectful and inclusive of all backgrounds and abilities
- Ensure activities are inclusive and flexible enough to meet the needs of children and vulnerable people
- Ensure programs that include children and vulnerable people who are Aboriginal or Torres Strait Islander, from culturally and/or linguistically diverse backgrounds or who have a disability, personnel will promote their safety (including cultural safety), participation and empowerment

Work health safety

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

All personnel are responsible for taking all reasonable steps to prevent workplace injuries or illness at work and cooperate with management in the best interests of health and safety and 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

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

All personnel will never humiliate, victimise, intimidate or threaten vulnerable persons or other workers in a direct or indirect manner.

All 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
- Gender or gender identity
- Sex or sexual identity
- Pregnancy
- Lawful sexual activity
- Impairment or disability
- Unrelated criminal record
- Religious belief or activity
- Physical features

Use of IT Resources

Use and ownership	TSA provides ICT resources to TSA personnel for the purpose of performing their role for the organisation. TSA retains ownership over the resources.
Right to monitor and review	TSA reserve the right to monitor and review the use of its ICT resources and to access all data on them. This includes, but is not limited to: ▪ Internet traffic ▪ Email messages ▪ Instant messaging ▪ Notebooks, desktops, mobile phones and tablets ▪ Encrypted traffic and information The use of ICT resources by TSA personnel constitutes consent to such monitoring and review.
Personal use	TSA personnel may occasionally use TSA resources, including ICT resources, for limited personal use, but this use must be 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	TSA 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 into the network (e.g. viruses, worms, Trojans, etc.) ▪ Accessing data or systems in an unauthorised way ▪ 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 approval
Defamation	TSA 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.

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). TSA personnel should not store TSA information in their notebooks or computers since it is not subject to information backups.
Personal information	TSA personnel are accountable and responsible for backing up any personal information stored on their notebooks or computers.

IT Asset Security

Cybersecurity	Everyone has an obligation to keep our ICT resources safe from viruses, malicious software programs and intrusion attempts. TSA personnel must not: ▪ Physically tamper any TSA issued ICT resources ▪ Disable the security software installed on an ICT resource or modify its configuration ▪ Modify the configuration of the operating system installed on an ICT resource
Cybersecurity incident	TSA personnel must immediately report any cybersecurity incident to the ITS Service Desk.
Unattended ICT resources	ICT resources must be secured or locked away when unattended to avoid theft. This also extends to locking computer screens.

User Accounts and Authentication Credentials

Responsibility	TSA personnel are accountable and responsible for all activity performed with their individually-assigned user account (or user ID) and ICT resources.
Personal use	TSA personnel must not use any issued user account (or user ID) or authentication credentials for personal use or to access other online services (e.g. Facebook, LinkedIn, eBay, Gmail, Hotmail, or a personal banking account).
Sharing of passwords	TSA personnel must not share or disclose their authentication credentials. Authentication credentials should be protected while they are being typed in to prevent shoulder surfing.

Password storage	TSA personnel must not write down authentication credentials in papers 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.
Breach/ disclosure	TSA personnel must immediately report any password breach or disclosure to the ITS Service Desk.

Removable Media

Use	The use of removable media 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 unless the media is encrypted. The ITS Department will assist with encrypting the media.
Security responsibility	TSA personnel are accountable and responsible for the security of the information they store in removable media and to comply with any applicable policies, procedures and regulatory requirements.
Hardware	Only ITS approved removable media hardware must be used to store sensitive and confidential TSA information. Personal removable media storage devices must never be used within TSA ICT environment.

Use of Personal Devices

Personal Mobile devices (BYOD)	TSA personnel who want to use their personal mobile devices (or BYOD) to store or access TSA information must allow TSA to install security software in order to protect TSA's information stored in the device. **This means the ITS Department will have visibility of the use of this phone, including personal use.**
Monitor and review	TSA reserves the right to monitor and review the use of mobile devices used to access TSA's information. Monitoring and review includes information stored on the phone and to track the location of the phone in case it is lost. **The use of corporate and personal mobile devices by TSA personnel constitutes consent to such monitoring and review.** When utilising encryption, TSA reserves the right to decrypt data as part of its monitoring efforts.
Personal information	TSA personnel are accountable and responsible for the security and backup of any personal information saved on BYO devices.
BYOD data wipe	TSA reserves the right to wipe, via remote access or otherwise, any TSA information (e.g. emails) stored on BYO devices.

Notebooks and Mobile devices

Security software	TSA personnel must not disable any security software installed on mobile devices once provisioned.
Application updates	Available software updates should be installed on mobile devices as soon as they are available.
Jailbreak / rooting	TSA personnel must not jailbreak or root an issued mobile device or their own personal devices (BYOD) used to store or access TSA information. Applications must only be installed from trusted sources (e.g. business catalogue or Android Play / Apple Store).
MMS, SMS and IM	TSA personnel must not use Multimedia Message Service (MMS), Short Message Service (SMS) or Instant Messaging (IM) to communicate TSA sensitive or confidential information.
Device wipe and collection	TSA reserves the right to wipe, via remote access or otherwise, any TSA issued notebook or mobile device; or collect such devices (1) upon termination of employment or service arrangement with TSA; or (2) at any time and without notice.
Personal information	TSA personnel are accountable and responsible for the security and backup of any personal information saved on notebooks and mobile devices.

Commuting and Travelling

Commuting and traveling	The nature of notebooks and mobile devices makes them a target for professional thieves. When travelling with notebooks and mobile devices, TSA personnel must always retain control over them. This includes: ▪ Not placing them in checked-in luggage ▪ Not leaving them unattended for any period of time TSA personnel are accountable and responsible for the physical security of notebooks and mobile devices.
Customs inspections	If TSA personnel are requested to decrypt a mobile device or media for inspection by customs personnel, 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	TSA personnel must not use TSA email services for sending 'junk mail', for-profit messages, or chain letters. Mass electronic communications should only be sent in accordance with TSA internal procedures.

Forwarding	Users may not setup 'auto-forwarding' of emails from their TSA email account to any external email address without prior formal approval from the IT department. This approval should be sought via a service desk request.
Confidentiality and privacy	Email is not a secure means of communication, particularly when used to communicate to external parties. TSA personnel must not use email to send sensitive or confidential TSA information to recipients outside TSA.  The ITS Department will provide advice on secure transmission of such information.

The Salvation Army Image

Use of branding	TSA is a well-recognised and respected organisation that projects a positive image to our recipients and the community we serve. 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. All personnel shall ensure their use of TSA's logo and brand assets complies with brand guidelines.
Public comment	Unless authorised in accordance with TSA's Media 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	All 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 individual ▪ Must not post any content that includes representation of children or vulnerable persons, without the express written permission from each vulnerable person and child, and the written permission from the child's parent or guardian Personal views are not to be presented as the position of TSA and must be clearly identified as a personal view. Content must not contradict TSA's Mission or Values.
Alcohol, smoking and non-medically prescribed drugs	Use of alcohol or any other substance must not adversely affect your work performance or the health and safety of others. Alcohol must not be consumed while on duty or at any meal breaks. Smoking is not permitted while wearing TSA branded clothes or while representing TSA, or in TSA buildings, vehicles or in the vicinity of entrances to TSA buildings. Alcohol and any other type of drug (legal or illegal) must not be supplied or used with any service recipient, irrespective of the service recipient's age. The manufacturing, distribution or use of a controlled substance is prohibited in the workplace or while conducting business on behalf of and in partnership with TSA. TSA recognises the need to respond sensitively to the needs of particular vulnerable groups, and exceptions to these rules may be considered with the approval and authorisation of applicable Senior Salvation Army Representatives.
Gambling	Gambling is contrary to the ethos of TSA and therefore raffles, sweeps or any other activity associated with gambling are not permitted on TSA's premises or when representing TSA.

Political affiliations and contributions	TSA maintains a position of political impartiality. All 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. The Salvation Army reserves the right to carry out a due diligence audit if it has any concerns in regard to the Suppliers compliance with Modern Slavery legislation.
Environment and sustainability	All personnel will strive to meet the highest environmental standards as stated in TSA's Environmental Sustainability Policy (GO_LR_POL_TEVS - *to be developed*).
Stewardship	All 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	All personnel will comply with all applicable minutes, codes, policies and procedures, and any reasonable directions by TSA.
Approved authorities	All approval and financial decisions must be made in accordance with TSA's Approved Authorities Policy (GO_LR_POL_TAAP).

Gifts and benefits	All personnel must not: ▪ Solicit any gifts or benefits of entertainment ▪ Accept offers of money or commissions ▪ Participate in any scheme in which a supplier offers incentives as reward for placing orders ▪ Accept offers or bribes ▪ Provide gifts, money or benefits of any kind to any service recipient, irrespective of the age of the service recipient Gifts and benefits are permissible in some circumstances, including: ▪ Sharing of low value gifts that would not be deemed to have an impact on engagement with TSA ▪ Gifts given or received as part of a pre-approved TSA initiative such as small low value Christmas gifts ▪ Any gifts received during the course of engagement from a service recipient, partner or supplier of low value if they are not deemed to have any adverse impact on TSA Low value is defined as a cumulative value over a twelve-month period being less than one hundred dollars. All gifts and benefits that are NOT low value must be recorded in a gifts and benefits register, which is maintained by the Governance and Risk office. Instances of attempted bribery must be reported to the Internal Audit Department, via the Head of Internal Audit, and in accordance with TSA's Fraud Control policy (GO_LR_POL_TFRC).
Purchasing and supplier management	All supplier selection, management and purchases must be in line with TSA's Procurement Policy (BS_FI_POL_TPRO) and Asset Management Policy (BS_FI_POL_TAMP – *to be developed*).
Conflict of interest	All personnel: ▪ Must disclose any actual, potential or perceived conflicts of interest ▪ Must report all conflicts or potential conflicts to the applicable Senior TSA Representative for assessment of the conflict ▪ Must remove themselves from the decision-making situations where the Chair of a meeting or other Senior TSA Representative has determined the conflict requires that action ▪ Will not engage in external employment where TSA has determined that a conflict of interest may arise, and the conflict is not able to be managed ▪ Must declare any personal relationships when in a decision-making position for purchases or supplier selection Details of any conflicting interests are to be reported to TSA's Governance and Risk office. Further detail on Conflict of Interest is available in the Conflict of Interest Procedure (GO_LR_PRO-02_TCOC – *to be developed*).
Secondary employment	Working outside TSA is permitted. Outside 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. Any additional employment which prevents or hinders or is in conflict with TSA should not be entered into.
Competition	All personnel shall not undertake work in competition with TSA or act in a manner contrary to their engagement obligations.

Information technology	Responsibilities for managing TSA assets, IT resources, Cyber security, physical security, data and access management must be in accordance with TSA's Information Security Policy (BS_IT_POL_TISP).
Knowledge, information and data management	Privacy, intellectual property, record keeping, corporate knowledge, data breach and confidentiality are managed by TSA in accordance with TSA's Knowledge, Information and Data Management Policy (GO_LR_POL_TKID – *to be developed*).
Theft, fraud and corruption	Any behaviour that is fraudulent, dishonest, corrupt or improper will be managed in accordance with TSA's Fraud Control Policy (GO_LR_POL_TFRC).
Whistleblower	All reporting of systemic wrong doing or disclosures of improper conduct within TSA must be addressed in accordance with TSA's Whistleblower Protections Policy (GO_LR_POL_TWBP).

Legislation

Compliance with laws	All 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 alleged illegal activities or conduct to the relevant authorities to the applicable Senior Salvation Army Representative
Compliance with integrity checks	All personnel must have relevant integrity checks such as police check and Working with Children/Working with Vulnerable Person Checks prior to engagement and at regular intervals in line with relevant state/territory legislation and TSA Recruitment and Onboarding policy (BS_HR_POL_TROB).

Roles and Responsibilities

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

Personnel	All personnel are required to perform their duties in line with this policy. Report any cyber-incidents and authentication credentials disclosure to the ITS Service Desk as soon as possible Protect ICT resources as per policy. Return ICT resources when required by ITS or when leaving the organisation.
Senior Salvation Army Representative	Ensures all personnel comply with this policy.

Risk and Compliance

The Code of Conduct Standard is approved by the Australia Territory Board that takes violation of this Standard seriously regardless of whether or not the actions in question were taken for the sake of convenience, or whether or not there is any actual loss or benefit to TSA or others.

Obligation	All personnel under the terms of their service, employment, engagement or contract must comply with all TSA policies, procedures and supporting documents. All personnel are required to read and acknowledge this Code of Conduct Standard as part of their induction to TSA, and every 2 years thereafter. Anyone who engages with TSA is expected to comply with this Code of Conduct Standard to the extent of their relationship with TSA.
Consequences of non-compliance	Failure to comply with this policy may result in disciplinary action or mediation and, in serious cases, termination of employment or engagement with TSA.

Location

Repository	Territorial Policy Application

Feedback

Feedback is encouraged	Feedback is used to improve and enhance the impact of this policy. It will be considered when reviewing and updating the document.
Who is feedback provided to?	All feedback is to be forwarded to Head of Governance and Risk via email to policy@salvationarmy.org.au.

Related Documents and References

Related Policy Documents	Approved Authorities Policy (GO_LR_POL_TAAP) Code of Conduct Policy (GO_LR_POL_TCOC) Conflict of Interest Procedure (GO_LR_PRO-02_TCOC) Incident Management Policy (GO_QA_POL_TCIM) Duty of Care Policy (GO_LR_POL_TDOC) Fraud Control Policy (GO_LR_POL_TFRC) Information Security Policy (BS._IT_POL_TISP) Knowledge, Information and Data Management (GO_LR_POL_TKID) Recruitment and Onboarding (BS_HR_POL_TROB) Remuneration and Conditions Policy (BS_HR_POL_TRAC) Safety and Wellbeing of Children and Young People Policy (GO_LR_POL_TSWC) Whistleblower Protections Policy (GO_LR_POL_TWBP) Work Health and Safety Policy (GO_WH_POL_TWHS)
Related Legislation	N/A
Funding Agreement Requirements	N/A
Governance/ Accreditation/ Certification Standards	N/A
Audit Report Findings	N/A
Other Relevant Documents /Resources	N/A

Document Control Information

Document ID	GO_LR_PRO_TCOC
Theme	Governance
Category	Legal, Risk and Compliance
Policy Owner	Assistant Chief Secretary
Policy Implementer	Head of Governance and Risk
Approval Authority	Australia Territory Board
Review Date	N/A
Next Review Date	June 2020
Previous Documents	**AUE** former Code of Conduct (June 2017) **AUS** former Code of Conduct (HR 2.1)

Document History	**Version**	**Date Approved**	**Summary of Changes**
	1-0	08/08/2019	Inaugural version