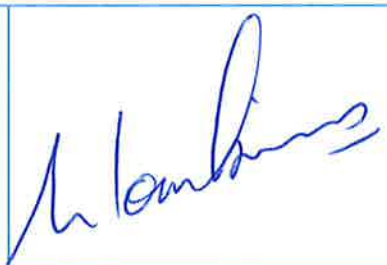
PROCEDURE

Office Security

Issued with the authority of the Chief Commissioner
and Chief Executive Officer of Scouts Australia NSW

Chief Commissioner signature		Chief Executive Officer signature	
Sponsor	Head of Risk		
Document type	Procedure	Date of issue	17 October 2018
Document code & no.	PRO 32	Version number	1.0
Document title	Office Security	Due for review	October 2021

Office Security

Contents

1 Purpose and scope

Scouts NSW will manage office security to help protect personnel from harm and property from theft. This procedure outlines the security practices State Office, Region Offices and office areas located at State Activity Centres.

Scouts Australia NSW is a volunteer organisation that has paid workers and subsequently, has responsibilities under WHS laws. Our volunteers are called workers under WHS laws and they have the same WHS obligations as a paid worker. Therefore, Scouts Australia NSW WHS Procedures apply to workers, members and volunteer supporters (which are all described collectively in the WHS Procedures as *workers*).

2 Office security risk assessment

The site manager is responsible for assessing security risks in consultation with workers and other stakeholders. At region offices, the region office manager shall assess security risks and seek assistance from their Region Commissioner and /or management at State Office if needed.

Risk assessments must be conducted in consultation with workers and other stakeholders in order to find solutions that are effective and acceptable. The risk assessment should cover, at minimum, the topics that appear as sub headers in this procedure.

Access arrangements should be determined on balance between *convenience* (for workers and visitors) and *security* (against unauthorised entry). Vulnerable access points should be identified relative to the specific location and layout and potential solutions put in place eg door locks installed, good lighting etc. Similarly, security risks relating to access to the surrounding carpark, bathrooms etc are also considered.

Security risks should be assessed and resolved prior to making any change that could impacting security. eg modifications to reception layout, changes to locking mechanisms or access policies etc. Similarly, events or changes that are outside the control of Scouts NSW might trigger also a review. Events that involve heightened security threats such as local protesters, recent crime in the area, renovation work might require additional temporarily security arrangements to be put in place. Similarly, modifications made by the landlord with or without consultation with Scouts NSW may require a permanent or temporary change in security arrangements.

All potential access points should be considered i.e. both authorised and unauthorised windows and doors. Reasonable solutions should be implemented considering the likelihood of unauthorised access and the likely consequence of that unauthorised access occurring. Solutions

might include steps taken to prevent the unauthorised access, as well as mechanisms to limit risk should the unauthorised access occur.

Examples:

- Preventative action - lock doors at all times
- Assistance mechanism – training about responding to aggression.

Refer to *Appendix 1 – Guidance notes for responding to an agitated caller or visitor*

3 Access to state office

State Office occupies a tenancy and like all other tenants, uses a swipe card system to control access. Member services manage the issuing of the swipe cards to staff and authorised members. Managers, via the Exit Checklist (or equivalent) should make every effort to retrieve swipe cards from terminating staff on their last day. In addition, IT must be advised immediately to de-activate any lost or unreturned card.

Holders of swipe card must not place any information on their card that would identify the organisation's name or address, as this is an obvious security risk.

When visitors will be present for a length of time that would require a swipe card (eg half a day or more) member services shall issue visitor swipe card during normal work hours. These visitor cards must be returned to reception at the end of each day / visit.

4 Personal security and phone threats

When a member of public makes a threat, it can lead to distress to staff members, in addition to the potential for the threat being carried out.

Refer to *Appendix 1 – Guidance notes for responding to an agitated caller or visitor* and *Appendix 2 – Aggressive confrontation checklist.* Staff who are most likely to receive a threat, such as Regional Office Managers, State Office Receptionist and Child Protection team members should be trained in procedures for responding to aggression and are to keep a copy of the phone threat checklist nearby. Completion of this checklist can assist police in identifying the perpetrator.

5 Protection of confidential information

Scouts NSW has responsibilities to protect the personal data of its staff, members and other stakeholders. Therefore, certain areas of the office should be treated as *out of bounds* for visitors,

6 Staff required to work alone

A risk assessment should be conducted where staff members are required to work alone, or where a staff member has expressed reasonable concern about their personal safety. Consider solutions such as personal duress alarms, mobile phone and pager, phone contact with a Security Guard and establish a means of communication. Ensure there is a process in place to address any emergency situations such as fire or medical emergencies and document in the Site ERP (Emergency Response Plan). Review how a single worker would deal with these situations compared to a group of people and implement process and training as required.

Ensure safe entry/exit, parking and adequate lighting is in place to reduce the risk for isolated workers arriving/leaving site. Review security at the location such as locks and gates and if the site is patrolled by a security service. Review if others could gain access to the premises and cause a safety risk.

7 Suspicious mail

Workers handling mail should remain vigilant and cautious at all times, but it should be remembered that most reports of suspicious packages are false alarms. Workers should have access to disposable Latex gloves and disposable plastic sealing bags.

Isolate the article and contact your Manager immediately with details. Manager to contact emergency warden and /or emergency services and obtain guidance on managing the situation and follow instructions given.

Wash your hands with soap and water as soon as possible. Manager or emergency warden o contact Site/Venue Manager if ventilation units /air-conditioning should be shut down.

8 Records & References

- Office Security Risk Assessments
- Training records
- Clean Desk Office Policy
- Data Breaches policy

9 Associated Forms

- H-S 23.1 New staff induction checklist
- H-S 32.1 Exit Checklist

10 Appendices

- Appendix 1 – Guidance notes for responding to an agitated caller or visitor
- Appendix 2 – Aggressive confrontation checklist

Appendix 1 – Guide to responding to agitated caller/visitor

All incidents are different so it is impossible to advise a specific process which should be applied in every situation. This guide describes the general recommended approach.

Key Factors

1. Stay calm
2. De-escalate the situation wherever possible
3. If the situation escalates, remove yourself from the immediate vicinity
4. Inform others of the situation and obtain help

1. Initial contact - Stay Calm

- Use a slow, low tone of voice
- Let the individual say what they need to say/blow off steam and avoid interrupting them
- Ask who they are and what outcome they are looking for
- Explain your role and what you are able to do for them
- Where you are unable to assist, explain you will go and locate someone who can
- If the person is aggressive or you feel threatened, skip to step 3
- **Your safety and wellbeing is the priority at all times**

2. Attempt to de-escalate the situation - determine next steps

- If they are there in person, ask them to sit down and wait whilst you find the appropriate person.
- If they are on the telephone, take down their name and contact number and ask them to hold.
- Seek assistance from your manager and /or co-workers as appropriate to determine next steps.
- If you can see they are upset/emotional, try and be empathetic without commenting on the problem itself – *"I can see that you are upset and I appreciate this is difficult for you. Perhaps if we take a moment we can try and find a solution together".*
- No worker is expected to accept aggressive behaviour from another person. Hanging up, leaving the room or directing them to leave are all options available to you where a person's behaviour becomes unacceptable.
- However there may be a point where you need to say: *"I find the manner in which you are speaking to me unacceptable. If you choose to speak with me calmly, I will try to assist you. Otherwise, I will end this call / direct you to leave".*

3. If the situation escalates - Remove yourself from the situation

If the situation escalates, you may remove yourself or hang up immediately:

- *"Unfortunately as you are no longer able to positively interact with me, I am no longer able to assist you. If you would like to leave your name and number I will ask someone to contact you, otherwise at this stage I will need to move onto other tasks"*
- Then hang up /leave the room. Alternatively, if you think the call should be traced, put the call on hold but do not hang up.

4. Inform others

- Alert your manager and inform reception or other staff who might receive further calls from the person. If the person was not identified, complete *Appendix 2 – Aggressive confrontation checklist* while it is fresh in your mind.
- Provide office staff with background information so that they are equipped should they need to handle any future calls from this person.

Appendix 2 – Aggressive confrontation checklist

After contact with an aggressor, complete this checklist while the incident is fresh in your mind. Each person who came into contact with the aggressor should complete their own form separately. This list should then be sent to the Child Protection Team or CEO.

Name of person filling out this form: Name of aggressor (if obtained):	Date, time, location of threat
Threat received / suspicious activity observed via: ☐Phone ☐ in person	Names of other colleagues present:
Description	**Describe the suspect**
What features does the suspect have	Examples
Does the suspect have an accent?	(American, Australian, Irish, British, Asian)
Does the suspect have a voice tone?	(Angry, child, calm, loud, soft, etc.)
Does the suspect have a speech impediment?	(Fast, slow, stutter, lisp, slurred, muffled, clear, etc.)
Does the suspect have strong threatening language / specific words	(Well spoken, taped, abusive, incoherent)
Does the suspect have any stand out descriptions?	(Tattoos, scars eye patches, height, clothing, shoes description)
How did the suspect leave?	(on foot, by car, alone, with an accomplice, which direction)
Continue to ask questions	**For example**
The more questions you ask, you can really get the answers you want from the suspect.	What is your name? Why are you doing this? What is wrong? (if all else fails) Do you know the police will soon be coming to get you?
After the conflict	
Report aggression to the highest member of staff currently present in the building and/or the police (000). Complete a Scouts NSW incident report form. If you continue to receive threats, report these too.	