Model Guidelines - Managing and Responding to Threats, Aggressive Behaviour and Violence from Members of the Public

June 2014

Acknowledgements

This guideline has been developed with reference to NSW Ombudsman office policies, and equivalent policies from other public sector agencies: in particular, NSW Housing's *Policy and procedures for the prevention and management of aggressive behaviour* (2001); the former NSW RTA's *Managing aggression and violent behaviour at work* (2002); NSW Parliament's *Guidelines for preventing and managing client aggression in electoral offices* (2001); and Centrelink's *Dealing with customer aggression* (2001).

NSW Ombudsman

Level 24, 580 George Street

Sydney NSW 2000

General enquiries: 02 9286 1000

Facsimile: 02 9283 2911

Toll free (outside Sydney Metro Area) 1800 451 524

Telephone typewriter: 02 9264 8050

Email: nswombo@ombo.nsw.gov.au

Web: www.ombo.nsw.gov.au

ISBN: 978-1-925061-31-4

Table of Contents

Model Guidelines - Managing and responding to threats, aggressive behaviour and violence from members of the public

Introduction

One of the most intriguing things about us is our diversity. Not only do we look different, sound different, come from different backgrounds and a range of experiences, we can also react very differently in certain situations.

This is not to say that any single response to a situation is right or wrong, however the unpredictable nature of human beings and their emotions can sometimes lead to unpleasant or even dangerous circumstances where the safety of one person is threatened by another.

Most organisations recognise that there is an element of risk attached to dealing with members of the public. My office regularly interacts with people who are frustrated, annoyed or angry with a certain situation, which is often when they are at their most volatile. Most of the time, this reaction comes from genuine concern and frustration and my staff are well trained on how to manage these situations in a way that is both fair and reasonable for all parties involved, including themselves.

These guidelines have been developed by my office to provide practical guidance to staff on how to deal with members of the public appropriately and safely. They outline what is expected of staff and the people interacting with them, as well as procedures for dealing with people who display threatening, aggressive or violent behaviour.

The guidelines are adaptable to a range of situations involving interactions between staff and members of the public. They also aim to support organisations in taking reasonable steps to ensure a safe working environment for their staff.

This is the first edition of our model guidelines on this topic. I hope they provide organisations and their staff with meaningful, practical support in the workplace.

Purpose

The [insert name of organisation] is committed to being accessible and responsive to members of the public. The [insert position title of the head of the CEO] is committed to ensuring all staff who interact with members of the public are aware of their responsibilities and are adequately supported in the event of unreasonable behaviour. This policy aims to balance public accessibility and staff security.

These guidelines provide practical guidance to staff on how to deal with members of the public effectively and safely. They outline what is expected of staff and the people interacting with them, as well as our procedures for dealing with people who make threats against themselves, staff or third persons, who display aggrieved behaviour or who are violent resulting in injury to people or damage to property. Debriefing after an incident and procedures for restricting access/contact or alternative arrangements for providing services are also addressed in these guidelines.

Responsibility

Management of security for [insert name of organisation] is primarily the responsibility of [insert title of security managers position], who reports to the [insert title of security committee].

The [insert title of position] is the security manager for the office who is responsible for:

- regular security audits of the reception area, interview rooms, counter area, alarm equipment, security procedures, and [insert names of any other locations, procedures or systems]
- managing or monitoring security related incidents
- investigating security incidents
- maintaining a register of security incidents
- educating staff in protective security measures

- advising and counselling staff, and
- keeping these guidelines and any related procedures up to date.

Staff are responsible for ensuring that they are familiar with these guidelines and any related procedures and put them into practice. Staff should report any security breaches, threats, aggressive behaviour or violence to the [insert title of security manager] and the [insert title of security committee].

Related policies and guidelines

This guideline should be read in conjunction with the [insert name of organisation] *Unreasonable Complainant Conduct Policy* and the *Managing Unreasonable Complainant Conduct Practice Manual, 2nd edition*, published by the NSW Ombudsman.

Definitions

Access restrictions and alternative service arrangements: **See 14 below.**

Anger: an emotion expressed through, for example, fury, resentment, wrath, vexation, acrimony and hostility.

Aggressive behaviour: unacceptably hostile behaviour towards staff or visitors to the office that creates an intimidating, frightening or offensive situation and/or adversely affects work performance.

Violence: behaviour that results in physical injury to persons or damage to properly.

Principles

The following principles should guide the responses by [insert name of organisation] to unreasonable behaviour involving threats, aggressive behaviour or actual violence involving members of the public:

1. the approach to be adopted by the [insert name of organisation], its management and staff in managing and responding to threats, aggressive behaviour and violence is to be in accordance with these written guidelines
2. the [insert name of organisation] will put in place appropriate security arrangements and equipment to protect the health and safety of staff from all reasonably anticipated threats, see **Annexure A** for a list of some of the arrangements and equipment that should be considered
3. staff are to make appropriate records addressing all actions taken following an incident involving threats, aggressive behaviour or violence and managers are to ensure that the decision-making process leading up to the imposition of any access restrictions or alternative service arrangements is transparent
4. a written record is to be made of every proposal to impose any access restrictions or alternative service arrangements, or where the assistance of police or mental health professionals has been sought, or a referral made to either for appropriate action
5. certain senior officers are authorised to make decisions to restrict a person's access to [insert name of organisation] premises or any of the services it offers or to impose alternative service arrangements in response to threats, aggressive behaviour or violence
6. staff are encouraged to explore the most appropriate access/contact restrictions or alternative servicing arrangements before deciding to withdraw face-to-face contact
7. staff are not to apply inappropriate access restrictions or alternative service arrangements to vulnerable people who have communication challenges arising from disability, geographical location, language barriers or educational disadvantage
8. appropriate monitoring/review mechanisms are to be implemented by relevant managers to ensure quality and consistency in the application of access restrictions and alternative serving arrangements
9. people the subject of access restrictions or alternative service arrangements are to be properly notified of their review rights and the review process, and given an opportunity to participate in and contribute to reviews wherever possible

10. any decision to limit or restrict access or impose alternative service arrangements should either apply for a definite limited time period, or be reviewed regularly to decide whether continued service restrictions continue to be necessary
11. training will be provided to relevant staff to ensure they are aware of the organisation's policies and guidelines for managing and responding to threats, aggressive behaviour and violence.

Model Guidelines

1. RESPONDING TO ANGER

Some of the members of the public who approach [insert name of organisation] may be frustrated, distressed or angry for a number of reasons. These factors can make it difficult for them to communicate effectively with us, and for us to understand and communicate with them. It may be that they are legitimately angry due to circumstances beyond their control, however intimidation, threats, aggressive or violence behaviour towards staff or visitors is not to be tolerated.

These guidelines provide managers and staff with information and strategies to help them deal with a range of inappropriate conduct by members of the public.

When people who interact with our staff are angry, in most cases this anger is directly related to the reason for the interaction or frustration they experience during that or previous interactions. They may perceive that they have been 'given the run around', or an unjust situation may have been created – or perceived to have been created – which is having serious financial, social or emotional effects on them. Their anger arises from frustration, annoyance or antagonism as a result of this real or perceived grievance.

Angry people have the same needs as anyone who approaches [insert name of organisation], but their anger can make effective communication with them difficult. It is important to attempt to manage their anger before turning to substance of their request, concern or complaint.

To effectively manage anger, you should first allow the person to express their frustration (to 'let off steam'). This will often mean the person will calm down enough to facilitate a focus on the actual cause of that anger or other substantive cause of their concerns.

When the person has calmed down, ask for more details or clarify your understanding of their issue(s) of concern. Allow the person to tell you about their issue(s) in their own words, and encourage them back to their point if they go off track. Repeat back to the person your understanding of their issue(s). You should be direct and clear about what you can and can't do, how long it will take and what it will involve, ensuring that the person participates as fully as possible in deciding how best to deal with his or her concerns.

Strategies for staff

Strategies staff should use when confronted by anger include:

- remaining calm and respectful – greet the person and preferably get them to sit down
- using a low, calm tone of voice and a slow pace
- listening – don't intervene too quickly and allow them a chance to 'let off steam'
- showing you are open to their point of view and using active listening skills (eye contact, nodding of head, open body position)
- acknowledging their anger without diagnosis, encouragement or criticism – feelings are real, even if you believe they are inappropriate
- paraphrasing and summarising what they are saying, picking out any key points and saying them aloud
- apologising without accepting blame – if any apology is deserved for some act or omission that is our responsibility, give one. If you or [insert name of organisation] is not at fault, you can still express sympathy with their feelings, eg *'I'm sorry to see that you are upset about what has happened'*
- agreeing with the person – without assuming any blame, listen for things you can agree with and express this. For example:

  'You're right, the Act does give you a right of objection'

  'I agree, it would be frustrating not to receive the information in time'

  'I accept that you are really disappointed with the service you received'
- not debating the facts while the person is still angry
- ensuring the person understands what you are saying – in particular, avoid jargon and legal language.

2. RESPONDING TO AGGRESSIVE PHONE CALLS

The same expectations about dealing with verbal abuse or personal menacing in face-to-face interviews apply to telephone calls to the office. It is clearly safer in a telephone call to inform the person you are talking to that you are willing to assist them but are not prepared to put up with verbal abuse, and will terminate the call if necessary. A person's behaviour on the telephone can always be made overt/explicitly labelled and limits set.

See also the *Managing Unreasonable Complainant Conduct Practice Manual, 2nd edition* for examples of aggressive phone calls and how to respond to them, and **6. Referrals of threats to self or third parties** above, for strategies to respond to threatening phone calls.

Strategies for staff

Strategies that can be used by staff to respond to aggressive phone callers include:

Step	Action
1.	Attempt to calm the caller.
2.	If this fails, inform the caller that you are unable to assist them while they are being aggressive. For example: *'I will end this call if we can't keep to the issues.'* *'I find the language and manner you are using unacceptable. If you continue to talk to me like this, I will end this call.'* *'I provided you with the information you require and if you have no new questions I'll end the call in order to deal with other people who are waiting.'*
3.	If the caller has been previously told only to contact the office in writing, they should be reminded of this and call ended immediately.
4.	If aggression continues, warn the caller again that you will hang up, mute the phone and seek assistance. **Put the receiver down but do not hang up.**
5.	If the abuse continues, the caller should be told *"I have told you I will hang up if you continued this behaviour. Goodbye.'* Then end the call. **Put the receiver down but do not hang up if you think the call should be traced.**
6.	Report the incident immediately by email to the receptionist and any other staff member who might take the call should the caller ring back.
7.	Discuss with your supervisor the options for dealing with further calls from the caller. These include: – you taking all further calls from the caller, – further calls being automatically put through to your voicemail, – another staff member taking any further calls, or – your supervisor taking any further calls.
8.	Inform reception what to do with any further calls.
9.	If the caller rings reception and asks to speak to your supervisor, this should only occur after reception has explained the situation to the supervisor and the supervisor has agreed to take the call. If the caller indicates that they wish to speak to the supervisor to make a complaint about the staff member who took their earlier call, they should be advised to put their complaint in writing to [insert titles of relevant position(s)].
10.	Make a note of the conversation on [insert name of relevant data base/case management system].
11.	Draft a memo and/or incident report for your supervisor recommending any further appropriate action.
12.	A completed Security Incident Report form should be emailed to the [insert titles of security manager and security committee].

3. RESPONDING TO THREATS, AGGRESSIVE BEHAVIOUR AND VIOLENCE

It is to be expected that some members of the public (particularly some complainants) will express a certain amount of anger. However, when this escalates into threats, aggressive behaviour or violence, a different management response is needed, centred on ensuring staff safety.

Threats and aggressive behaviour are more than anger or antagonism. They involve some verbal attack or intimidation that is harmful or offensive to the staff member involved. Violence can involve harm to individuals or damage to personal or office property.

Common causes of threats, aggressive behaviour or violence include:

- situational factors such as noisy waiting rooms or noisy office surroundings, delays in getting to speak to someone, fear of unknown people or a new environment, excessive heat, pain, emotion
- the belief that some form of wrong has been committed against them, such as having their property stolen or having someone jump ahead of them in the queue
- low impulse control
- difficulty verbalising problems, often resulting in feelings of being rushed or being unable to explain their problem properly
- medical illness, and/or
- the effects of drugs or alcohol.

Staff faced with aggressive behaviour need to be able to manage the situation effectively before they can deal with the actual issues of concern to the individual. You are not expected to continue dealing with threatening, aggressive or violent individuals. In particular, you should terminate an interview and initiate safety procedures in response to any physical violence, or threats thereof. Verbal aggression may also lead to you terminating contact, either for the short term or permanently, if the behaviour continues after you have tried to put the person at ease or calm them down. All incidences of aggressive behaviour must be reported to the [insert title of the security manager and security committee], see **Annexure B** for a Security Incident Report form.

One of the most important ways of avoiding aggressive behaviour or violence is to read the signs exhibited by the person. Some of these are very obvious and some less so. Your feelings are often a good indicator if the person you are dealing with is aggressive. What you choose to do about the emerging or existing aggressive behaviour will depend largely on where you think it is heading. This may be determined by whether the aggression is reactive or goal directed. If you can identify and deal with the causes of aggressive behaviour, you may be able to control the situation to a manageable level.

It is useful to distinguish between two types of aggressive behaviour:

- *Reactive behaviour* - stemming from fear, frustration or feeling under threat, and can be triggered by a noisy waiting room, a comment by the interviewer, or the accumulation of a number of frustrations. Reactive behaviour is not usually directed towards you and these are causes you may be able to control and ease the aggression.
- *Goal directed behaviour* - which might be directed towards staff to achieve a desired result. It may come from the belief that intimidation is the only way to achieve an aim. This is less likely to be behaviour you can influence.

Acknowledging and referring to the specific aggressive behaviour may stop aggression, particularly when it is followed by appropriate limits being set. You need to use your judgement as this approach may only add to a person's aggression.

The following signs or information may provide clues about the potential for a person to engage in aggressive behaviour or violence:

- appearance of intoxication or being under the influence of drugs
- bloodstained or dishevelled appearance
- pacing, agitation, tapping feet
- clenching of fists, jaws
- hostile facial expression
- increasing activity levels during the interview
- standing up frequently and entering off limit areas uninvited
- loud or slurred speech

- sarcasm, abusive swearing, threatening, caustic wit
- inflexibility
- irritable, anxious, short tempered, tense, distressed mood
- not in control of emotions
- a known history of violence.

Strategies for staff

Strategies for staff to deal with threats and/or aggressive behaviour include:

- continually assess the possibility of the situation becoming violent – are the signs abating or becoming worse?
- you may need to walk away – find an excuse to do this (eg check a file, get a letter)
- remember there is security in numbers – ask another staff member to accompany you
- take a step back to create space if you see signs of physical aggression
- maintain normal eye contact – deliberate eye-balling can seem very aggressive
- provide alternatives to the aggression by making it clear that their aggression will not achieve their goal
- be careful of not getting into a fight – remember your expert knowledge may be intimidating. Share this knowledge with them, be confident, but don't use these things to make the person seem inferior
- maintain non-confrontational body language – nodding and turning your ear toward the speaker are appropriate signs that you are listening and not playing for power. Keep your hands in front of you at waist level
- get something between you and them – a desk, a document, a list of proposed actions, something that you had both agreed on previously
- do not attempt to physically restrain any person or to physically intervene between other people who are behaving aggressively toward each other
- withdraw earlier rather than later and offer another time when you may feel better about talking to them
- don't be a hero.

See **Annexure C** for tips for responding to threats, aggressive behaviour and violence. **Note**: Copies of this Annexure should be separately handed to all front line staff.

Obtaining a statutory order to address threats, aggressive behaviour or violence

Where there is an ongoing cause of inappropriate behaviour by a person and you have a reasonable and genuine fear of actual or threatened physical violence, intimidation or stalking, another option to consider is whether to seek a statutory order from a court to restrain such conduct. See Annexure D for advice about this option.

Restricting access to our premises

Another option that might be appropriate, in particular to address actual or threatened violence or a course of conduct that is causing distress to staff, is to restrict access over our premises. See **Annexure E** for advice about this option.

4. RESPONDING TO MAIL AND BOMB THREATS

All staff should be vigilant when handling mail or packages. If any mail or its deliverer seems suspicious, do not touch it. Check with any named recipient as to whether they are expecting a package.

Also consider contracting the sender, if identified, and ask if they sent the item. If you are still suspicious, inform your supervisor and the [insert title of security manager]. **See Annexure F** for more information.

If you receive a bomb threat by phone, **put down the phone but do not hang up**. Make notes of all relevant details to enable appropriate information to be given to the police. The information can also be used to develop a risk assessment plan to deal with the situation. If you suspect an item is a bomb, do not touch it. Contact your supervisor and the [insert title of security manager] immediately. They will decide if any of the following people need to be notified:

- the [insert titles of Business Continuity Manager (BCP manager), security manager and security committee]
- [insert building/office security staff - if any]
- the staff member who is the Floor Warden
- the Chief Warden for the building.

The Chief Warden is responsible for advising the Police and liaising with the [insert BCP manager] and [insert title of security committee] to assess the seriousness of any bomb threat and make a decision as to what action should be taken. This may include searching the building for the bomb and/or evacuating the building. If it is not clear that the [insert BCP manager] or Chief Warden has advised the Police, your supervisor and the [insert title of security manager] should do so and advise the [insert BCP manager] and [insert title of security committee].

In the event of an evacuation, follow emergency evacuation procedures. Stay calm and alert during the evacuation and assemble in your designated area. Floor wardens will advise when it is safe to return to work. The police contact for bomb threats is the [insert details of police contact and phone number].

See **Annexure F** for more information about how to deal with suspect mail and **Annexure G** for information about responding to bomb threats.

5. RESPONDING TO THREATS WITH A WEAPON

Where any member of staff or visitor is threatened with a weapon, or it is reasonably suspected that this is about to occur, the police must be called immediately.

See **Annexure H**, for more information about dealing with threats with a weapon.

6. REFERRALS OF THREATS TO SELF OR THIRD PARTIES

While it is not our role to make psychiatric assessments or to provide social work services, we do occasionally come across cases where it may be negligent to do nothing. Threats of self-harm, suicide or violence by members of the public should be taken seriously.

Consideration may need to be given to contacting police or any relevant mental health response team, or for that matter any other relevant person or body, to pass on information that relates to or is necessary to prevent harm – including self-harm – to any person.

Strategies for staff

Strategies for staff to respond to phone calls where threats of self-harm or harm to third parties are made include:

Step	Action
1.	If a person threatens to harm themselves or another person, do not aggravate the situation by responding in an authoritative way or by appearing unsympathetic.
2.	Advise the person making the threat that it is the policy of [insert name of organisation] that you must report such matters.
3.	Discuss any threats of harm to self or others immediately with [insert title of relevant officer(s)].
4.	With the approval of one of these senior officers, disclose any appropriate information to police or other relevant persons or bodies if you believe that doing so is necessary to reduce the likelihood of harm occurring.
5.	Inform your supervisor.
6.	A completed Security Incident Report form must be emailed to [insert titles of security manager and security committee].

7.	If requested by the [insert titles of the security manager and security committee], collect accounts of what took place from any witnesses listed on the security incident report.
8.	If a staff member is injured in any way as a result of the incident, they or their supervisor must complete and submit a [insert title and details of how to find a form to notify injury/illness], which are available from Personnel.
9.	The [insert titles of security manager and/or security committee] should liaise with Personnel to determine whether the incident should be reported to WorkCover.
10.	Place all relevant documents on the [insert titles of relevant incident/injury register, workers' compensation type files] and any file kept in relation to the person concerned. Copy details of any incident that occurs in a public contact area to [insert titles of the security manager, security committee and any other relevant officer].

Strategies for supervisors to respond to threatening phone calls made to staff include:

Step	Action
1.	Ensure that the [insert title of relevant positions] have been informed and a completed Security Incident Report form has been emailed to [insert titles of security manager and security committee].
2.	Inform staff member of the various options available to provide them with support (*see 12c Other remedies* below for more information).
3.	Monitor the staff member (especially where no support options have been exercised).
4.	Liaise with the [insert titles of relevant office manager and security committee] about the need for an operational debrief, see **Annexure K** for more information.

7. SECURITY IN PUBLIC CONTACT AREAS

7.1 Risk Management

The [insert title of security manager] is responsible for conducting six monthly inspections of all areas of our premises where staff come into contact with members of the public, focussing on safety issues. A report outlining the results of each inspection is to be provided to the [insert title of security committee].

See **Annexure I** for a list of factors that to be considered when conducting a risk assessment of public contact areas.

7.2 Reception/waiting area

The layout of the reception area interview counter and interview rooms should take into account the needs of both staff and visitors.

No visitor is permitted access to secure staff work areas unless they are signed in accordance with the security policy or in exceptional circumstances.

See **Annexure J** for key factors impacting on physical security in the reception/waiting area.

7.3 Interview rooms

It is mandatory [or advisory] for staff to take a duress alarm when interviewing a member of the public in any enclosed interview room. Duress alarms are available at [insert location of duress alarms].

Members of the public should not be taken into an interview room unless they are calm and composed.

Reception staff [or insert other relevant position] must regularly check that interviews are proceeding without incident, and must immediately report any concerns they may have to [insert title of relevant position]. If an interviewing officer is concerned an aggressive incident may occur, they should leave the door to the interview room open.

Seating arrangements in interview rooms should allow both the interviewer and the interviewee easy access to the door, as well as providing some protection for the staff member if the interview deteriorates. The table should always be placed between the interviewer and the interviewee. Staff conducting an interview should take the seat closest to the door.

The [insert titles of relevant officers] are responsible for ensuring that information about interview room layout, exits and location of duress alarms is provided during induction and training of new staff whose duties may involve direct interaction with members of the public. New staff should familiarise themselves with this information.

8. ADMISSION OF VISITORS TO SECURE PREMISES [WHERE SECURITY DOORS CONTROL ACCESS TO PREMISES]

Reception staff are the first point of contact for members of the public attending our office. No other staff members should admit any visitor to secure premises unless they know them. All visitors must be directed to [include details of identification and authorisation arrangements].

Strategies for staff

Strategies for staff to control admission into the premises through security doors include:

Step	Action
1.	Staff are not to admit visitors through the security doors into the reception area if they consider this may be unsafe, in which case the intercom should be used to ask them to identify themselves and why they have come to the office. Entry should only be permitted when staff have no remaining safety concerns – usually after checking [names of databases, including case management systems, incident registers, files, etc] to clarify the visitor's status, and/or speaking to supervisors to clarify.
2.	If the person at reception has had limits imposed on the matters that [insert name of organisation] will deal with, the staff member dealing with the person must decide whether they believe they can explain this and then request the person leave the premises. If possible, photocopy the letter of restriction to hand to the person: the [insert title of security manager] is responsible to keep copies.
3.	If the person is known to have been informed that they are not to enter the premises, or it is otherwise considered to be inappropriate to allow their entry to the office, staff do not have to admit them to the reception area. Instead, staff can be informed via the intercom that they will not be admitted or a more senior officer can be asked to attend to speak to the person outside the office door.
4.	If the person refuses to leave, contact the [insert title of relevant positions] and [insert building/office security – if any] for assistance. If they are not available, seek assistance from [insert title of security manager].
5.	If the person at reception has not had their contact restricted, contact the staff member responsible and ask them to attend the reception area. If they are not available, contact their supervisor to arrange another interview.

9. INTERVIEWING MEMBERS OF THE PUBLIC

9.1 General procedures

Members of the public who indicate an intention to attend at the office or who have regular dealings with [insert name of the organisation] should be encouraged to make an appointment as this allows time adequate preparation for the appointment or interview. However, it is the policy of the [insert name of organisation] that appropriate staff will [or will not] see people who drop in unannounced.

All interviews should be completed by [5.00pm or the close of business]. If an interview or meeting is likely to finish later than [the close of business], you should inform your supervisor and reception to ensure that any potential security issues are addressed.

You should avoid arranging interviews to start before 9.00am. If an interview starts before 9.00am, you must ensure you have a duress alarm with you.

You should only meet with a person you do not know between 9.00am and [the close of business].

Before starting an interview, you should make sure you have checked records kept by [insert name of organisation or relevant business unit] about any previous incidents of inappropriate behaviour that may have involved that person, including any history of threats, aggressive behaviour or violence.

The [insert name of organisation or relevant business unit] maintains a separate file of security incidents that may be checked on request, subject to confidentiality requirements. If you have any concerns about the potential for inappropriate behaviour, you should inform your supervisor and the [insert title of security manager] about where and when the interview will take place. You should take another staff member to the interview as backup.

If you are concerned for your safety, you are not obliged to conduct an interview on your own. You can always call on another staff member to provide assistance. [All staff interviewing a member of the public in an interview room must collect an interview folder from [insert location of folders] prior to entering that room. This file contains a duress alarm, paper, list of key 'do's and don'ts' of interviewing, a referral list and office brochures. If the staff member forgets, the receptionist should interrupt the interview to request that the staff member collects the folder.

Strategies for staff

Strategies for staff when interviewing members of the public in an interview room include:

Step	Action
1.	For known customers/clients/complainants/etc, check [name of relevant data base(s)] for most recent correspondence to ensure you are familiar with the particular matter.
2.	Collect folder with duress alarm, before accompanying the person to an interview room.
3.	Ensure that you are sitting at the designated interviewer seat and that the interviewee is sitting across from you on one of the other chairs. Ensure you both have access to the door.
4.	At the conclusion of the interview, escort the person to the lift. If difficulties arise, ask the receptionist to call another staff member to assist.
5.	In the event of an interview breaking down (eg because the interviewee is behaving aggressively, the interviewer feels threatened, etc), there are four possible options for interviewer: • attempt to continue the interview with a warning • interrupt the interview by excusing yourself (eg to check some information/get a pamphlet) • end the interview without using duress alarm • end the interview using duress alarm. See 'What to do when an interview breaks down' below for more detail on each of these options.

9.2 What to do when an interview breaks down

There will be situations where you are unable to address a person's concerns. In a small number of cases, this can result in a person becoming aggressive towards a staff member. Interviews should only be terminated if you feel threatened, or after you have made reasonable attempts to calm the person.

Strategies for staff

Strategies that can be used by staff when an interview breaks down include:

OPTION 1: Continue interview with a warning/interrupt interview

Step	Action
1.	Warn the interviewee that if he/she does not cease the behaviour you will have to terminate the interview. For example: *'I will have to end this interview if we can't keep to the issues.'* *'I find the language and manner you are using unacceptable. If you continue to talk to me like this, I will end the interview.'*
2.	If the interviewee continues the behaviour, exercise one of the following options: • end the interview, possibly with an offer to reschedule for another time • interrupt the interview and ask the [insert title(s) of security manager and/or any other relevant position(s)] for another staff member to assist or take over.
3.	After the person has left, a completed Security Incident Report form must be emailed to the [insert titles of security manager and security committee].

OPTION 2: End interview without use of the duress alarm

Step	Action
1.	Warn the interviewee that if the behaviour does not cease, you will have to end the interview. For example: 'I *will have to end this interview if we can't keep to the issues.'* *'I find the language and manner you are using unacceptable. If you continue to talk to me like this, I will end the interview*.'
2.	If the interviewee continues their behaviour, seek backup from the [insert titles of security manager and relevant positions]. Note: Staff are not expected to tolerate aggressive behaviour.
3.	End the interview.
4.	After the person has left, a completed Security Incident Report form must be emailed to the [insert titles of security manager and security committee].

OPTION 3: End interview using the duress alarm

Step	Action
1.	If time permits, warn the interviewee that if he/she does not cease the behaviour you will end the interview. For example: *'I will have to end this interview if we can't keep to the issues.'* *'I find the language and manner you are using unacceptable. If you continue to talk to me like this, I will end the interview.'*
2.	Press the duress alarm.
3.	Retreat from the interview room or the counter into the secure office area.
4.	If retreat is not possible, you are entitled to use reasonable force to defend yourself. Reasonable force is the amount of force necessary to stop an attack or prevent personal injury – nothing more.
5.	Seek support from your supervisor and/or the [insert title of security manager]. Reception will alert these staff to any incident.
6.	After the incident, a completed Security Incident Report form must be emailed to the [insert titles of security manager and security committee].

10. USE OF DURESS ALARMS

There are duress alarms at [identify locations of fixed duress alarms].

There are also portable duress alarms for use in the interview rooms. All staff interviewing members of the public in interview rooms must take alarms with them.

Drills in the use of and response to alarm and security systems should be undertaken every six months.

It is the responsibility of the [insert title of security manager] to organise these drills and the responsibility of the [title of security committee] to ensure this is done.

You should activate a duress alarm if you feel threatened and you cannot take other action to address the situation (eg taking a break to seek advice or assistance), when a person refuses to leave the premises when asked, or in a case of physical aggression or property damage.

[There are two levels of alarm and response, local (blue button) and office-wide (red button):

the local alarm sounds on [identify location]. The [identify relevant positions] will respond and provide assistance and direction as required.

the office-wide alarm sounds throughout the office. All staff from [specify which staff or positions] must respond.

Strategies for relevant staff

In the event of a duress alarm being used [specify which staff or positions] should respond immediately in accordance with the procedures outlined below:

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1.</td><td>Go immediately to the reception area [or the relevant public contact area] when the duress alarm sounds.
Other staff members – in consultation – should decide whether they are required.</td></tr>
<tr><td>2.</td><td>One person, usually the most senior staff member, is to take control.</td></tr>
<tr><td>3.</td><td>Arrange for someone to stand next to a phone or duress alarm that connects to either the police or [insert building/office security if any].</td></tr>
<tr><td>4.</td><td>Assess the situation by looking into the interview room/public area.</td></tr>
<tr><td>5.</td><td>If you are not sure that an incident has occurred (it may be a false alarm), knock on the door and advise the staff member that you have an urgent phone call for them. When the staff member steps outside, shut the door and move away from the interview to discuss the situation.</td></tr>
<tr><td>6.</td><td>If the level of harassment is medium (raised voices, low-level threats), provide assistance for as long as possible without endangering yourself.</td></tr>
<tr><td>7.</td><td>If an incident is occurring, ask the person to leave. If they refuse, ask the [specify titles of relevant positions] to call [insert building/office security if any] and/or police.
If a violent incident is occurring, the police should be informed immediately, as well as senior management:
Emergency contact numbers
<table><tr><td>Emergency</td><td>000</td></tr><tr><td>Police</td><td></td></tr><tr><td>Building/Office Security</td><td></td></tr><tr><td>Floor Wardens</td><td></td></tr><tr><td>First Aid Officers</td><td></td></tr></table></td></tr>
<tr><td>8.</td><td>Ensure no one blocks the exits, and that there is an avenue of escape for the aggressor.</td></tr>
</table>

9.	Consider whether it is necessary to remove any bystanders from the area either by the lifts or if this is not possible, into one of the hearing rooms, locking the doors behind you.
10.	When [building/office security - if any] and/or the police arrive, the most senior officer present should remain – all other staff should return to the secure area.
11.	Organise medical treatment for any staff member or visitor who requires it.
12.	All involved staff should complete a Security Incident Report form, which must be emailed to the [insert titles of the security manager and security committee]. Staff should then be debriefed by another senior staff member.

11. INAPPROPRIATE WRITTEN CORRESPONDENCE, INCLUDING EMAILS

The problems that arise in oral communication may also arise from time to time in written communications. The response will depend on the level of concern.

Any actual or reasonably suspected threat must be immediately notified to the [insert titles of security manager and security committee], as well as your supervisor.

Staff should discuss with their supervisor how best to manage the person's conduct. Relevant guidance can also be found in the *Managing Unreasonable Complainant Conduct Practice Manual, 2nd edition.*

Note: Correspondence containing very inappropriate language can be returned to the writer with advice that we will assess the requests or issues they wish to make or raise when more appropriate language is used.

12. POST INCIDENT RESPONSIBILITIES

Any incident of aggression should be reported to the [insert titles of security manager and security committee] as soon as possible and within 24 hours if you are away from the office. If an assault occurs, supervisors are responsible for ensuring first aid and/or medical treatment is provided to any staff member or visitor requiring assistance. All major assaults should be reported to the police.

A completed Security Incident Report form must also be submitted to the [insert titles of security manager and security committee] within 24 hours. If the injured person is unable to complete the form, the relevant supervisor, [insert titles of other relevant positions] must complete the form in as much detail as possible. The [insert title of security manager] is responsible for providing staff with any assistance they may need in dealing with police.

12.1 People's reaction to stressful situations

Dealing with people who are very demanding, abusive aggressive and/or violent can be extremely stressful and, at times, distressing or even frightening. It is perfectly normal to get upset or experience stress when dealing with difficult situations. Everyone reacts differently to stressful events.

Stress can be cumulative, often resulting in a strong reaction to a minor event which forms part of a chain of stressful events.

Signs of stress can include:

- physical signs such as shock, nausea or fainting immediately after an event, or long term aches, pains and fatigue.
- emotional responses such as anger, fear or depression – this is often reflected by crying or feeling tearful. Difficulty in thinking clearly, making decisions or concentrating on the job.
- behavioural changes such as increased irritability, withdrawing from people, insomnia, nightmares or resorting to alcohol more frequently or in greater quantities.

Recognising signs of stress in yourself and others is an important step in dealing with the problem. The [insert name of organisation] has a responsibility to support staff who may experience stress as a result of situations arising at work.

12.2 Debriefing

Debriefing means talking things through following a difficult or stressful incident. It is an important way of 'off-loading' or dealing with issues. It is usually voluntary, with the exception of operational debriefs, and can occur in a number of different ways.

All staff can access the Employee Assistance Program – a free, confidential counselling service. To make an appointment, call [insert number of EAPs provider]. For traumatic incident or crisis counselling, call [relevant number]. Brochures about this service are available from Personnel, and [specify locations]. Information is also available on the office intranet under [specify location].

See **Annexure I** for more information about debriefing following an incident.

12.3 Other remedies

(a) Compensation for injury

Any staff member who suffers injury as a result of aggressive behaviour from complainants is entitled to make a workers' compensation claim. Personnel will assist wherever possible in processing your claim. If you are the victim of an assault, you may also be able to apply to the Victim's Compensation Tribunal [or equivalent] for compensation.

(b) Compensation for damage to clothing or personal affects

Where damage is suffered to clothing or personal effects as a result of aggression by a member of the public in an employment related situation, compensation may be sought.

For more information, see [insert name of organisation] policy [insert title of policy covering the payment of compensation to staff for loss or damage to private property].

(c) Legal assistance

If a staff member is physically attacked, or is a victim of employment related harassment by a member of the public, and the police do not lay charges, the [insert name of organisation] will consider providing reasonable legal assistance if the staff members wishes to take civil action.

(d) Threats outside the office or outside working hours

Where threats are directed at a particular staff member and it appears those threats may be carried out outside normal working hours or outside the office, the staff member will receive the support of the office. Requests for such assistance should be made to your [insert title of relevant manager positions].

(e) Escorts home

When a staff member fears for their safety following a threat from a member of the public who they have previously dealt with, or are currently dealing with, another staff member may accompany them home or the [insert name of organisation] can meet the cost of the staff member going home in a taxi.

Ask your [insert titles of relevant manager positions] for more information.

(f) Telephone threats on home numbers

If a staff member or their family have been harassed by telephone at their home and they believe it is connected with their employment with the [insert name of organisation], they may apply to have the office meet the cost of having their telephone number changed and/or made silent. The staff member should also contact their telephone carrier, as they may provide an interception/monitoring service.

If assistance is approved, the [insert name of organisation] will meet the cost incurred for a period up to 12 months. Once approval is given, the staff member is responsible for making the necessary arrangements and will be reimbursed after producing a paid account.

Applications for reimbursement must be approved by the [insert title of security committee].

(g) Other security measures

If other security measures are necessary, the [insert name of organisation] will give consideration to providing all reasonable support to ensure the safety and welfare of the staff member.

13. REPORTING REQUIREMENTS

All serious incidents involving personal abuse, threats of violence or actual incidents of violence should be reported on a security incident report form to be maintained in a register by the [insert title of security committee]. This provides a source of documentation for any action needed, as well as allowing the [insert name of organisation] to identify any trends and take remedial or preventative action.

See **Annexure B** for the Security Incident Report form, which can also be accessed on the Intranet at [location of document].

14. RESTRICTING ACCESS OR IMPOSING ALTERNATIVE SERVICE ARRANGEMENTS

14.1

Some people will not be satisfied with the action we take. They can be extremely persistent and cannot or will not accept that we are unable to assist them further and/or disagree with what we have done in relation to their issue, request, application, complaint, etc. A small number are also so aggressive and/or abusive that we are forced to only deal with them in writing. Such people pose a potential threat and/or tend to consume a disproportionate amount of the [insert name of organisation]'s time and resources.

We need to use resources efficiently and effectively and to take appropriate steps to ensure staff safety. We will review a person's interactions with the [insert name of organisation] and our staff if we believe their behaviour unreasonably uses our resources or threatens staff safety.

These situations are the exception rather than the rule. Letters informing a person of decisions to restrict their access/contact, or the imposition of alternative service arrangements must be approved and signed by the [insert title of CEO, or relevant senior/office manager position(s) with authority to make such decisions].

14.2 Restricting access or imposing alternative service arrangements

A restricted access or alternative service arrangement decision can be made where a person's conduct is deemed so unreasonable (eg threatening, aggressive, abusive, violent, etc) that the [insert title of CEO, or relevant senior/office manager position(s) with authority to make such decisions] decides to restrict all their contact with [insert name of organisation].

The following are some common examples of the access/contact restrictions that can be applied:

- only in writing via the postal system
- only by telephone
- only with a specified officer
- only by telephone or with a specified officer at a specified time
- only in relation to a new matter/application/request, etc
- only in a room monitored by CCTV, or
- a combination of any of the above.

The following are some examples of alternative service arrangements that might be applied:

- conditional service agreements (eg agreements that a person will meet certain obligations or refrain from certain conduct in return for the continued provision of a service, or its continued provision at a certain place or in a certain way, etc)
- service only being provided on-line or by correspondence and not face-to-face
- a service only being provided by a specified unit of or person within the organisation (ie a unit or person with the necessary skills, experience, access to resources, etc, necessary to adequately deal with the types of behaviour engaged in by the person concerned)

- a service only being provided from a particular location (eg premises with greater security than the standard premises of the organisation [if any], or from another organisation that operates out of premises with greater security)
- a particular service only being provided at the home of the person if in the presence of (and subject to the availability of) an advocate/support person, specified family member, an additional staff member, the police, etc
- a service only being provided via an advocate/support person or family member
- etc.

Any restriction or alternative service arrangement must be reviewed periodically in accordance with these guidelines.

Strategies for staff

Strategies to be adopted by staff in relation to restricted access and alternative service arrangement decisions include:

Recording restricted access and alternative service arrangement decisions

Step	Action
1.	Draft a statement of reasons in support of a recommendation to your supervisor and the [insert title of relevant office manager position] that a person's access should be restricted or an alternative service arrangement put in place.
2.	Gain approval of your supervisor and the [insert title of relevant office manager position].
3.	Draft a letter for the signature of the [insert title of CEO, or relevant senior/office manager position(s) with authority to make such decisions] that clearly explains: • the behaviour which led to the restriction in services • why the behaviour was not appropriate in the circumstances • the nature of the restriction or an alternative arrangement being put in place • the duration of the restriction/arrangement • how the person may contact the organisation, including the name and address of a nominated contact officer • how the person may make a complaint to the organisation about any future service delivery problems • how the person may request a review of the decision.
4.	When the decision is made, send the signed letter to the person by mail or email.
5.	Email a copy of the signed letter to the [insert title the relevant office manager position] who will notify relevant staff of the details of the decision.
6.	Email a copy of the signed letter to the [insert title of security manager].
7.	Save a copy of the letter to the relevant [insert details of the locations where copies of the letter should be saved] and also place a hard copy on [insert details of any relevant hard copy file - where relevant].
8.	The [insert title of relevant office manager position] is to enter the restriction on the *Restricted Access List* and amend the person's file [if there is one] to show *'Restricted Access/Alternative Service Arrangement'* in the [insert location/field].

9.	The [insert title of relevant office manager position] will also advise IT if the restriction involves blocking the person's emails. IT are authorised to take the relevant steps to block a person's emails upon receipt of such advice and to cause an automatic reply to any further emails from the person stating *"Your email was blocked for reasons the [insert name of organisation] set out in its letter to you of …. date. You will receive no other reply to this email.'*
10.	The [insert title of relevant office manager position] will record the review date on the *Restricted Access and Alternative Service Arrangement Review Schedule.*

14.3 Reviewing restricted access and alternative service arrangement decisions

Actions to be taken to have restrictions and alternative arrangements are regularly reviewed include:

Step	Action
1.	The [insert title of relevant office manager position] and the [insert title of security manager] must review restrictions as required by the Restricted Access and Alternative Service Arrangement Review Schedule.
2.	The reviewing officers must consider any subsequent incident(s) or failures to comply with a restriction. Generally restrictions and alternative arrangements should be lifted or relaxed: • unless staff have evidence that the continuation of the restriction or arrangement is clearly necessary, or • where the conduct involved serious violence or a course of conduct involving threats or abusive behaviour, the restriction or arrangement should remain in force until the person concerned can demonstrate that they are no longer a threat.
3.	The [insert title of CEO or relevant senior/office manager position(s) with authority to make such decisions] must approve extending the time period of a restriction. The person the subject of the restriction should be notified of the extension, unless there is a good reason not to.

ANNEXURES

Annexure A - Security arrangements and equipment

Organisations need to consider the types of security arrangements and equipment they need to have in place to ensure the safety of staff whose duties involve dealing with the public.

- security related equipment or fixtures that should be considered include:
- security doors controlling access to premises
- 'escape avenues' for staff working in public access areas (such as escape doors located behind reception counters)
- CCTV cameras covering all public contact areas (with appropriate signage to: comply with any legal requirements; act as a warning to people considering behaving inappropriately; and to obtain evidence that might be used to support any decisions to restrict access, etc, or in any subsequent legal proceedings)
- monitors showing what is being filmed by the CCTV cameras (such screens should be visible to relevant supervisors and the people in the public access areas covered by the cameras)
- duress alarms both fixed alarms in appropriate locations and mobile alarms that staff can take with them into interview rooms or other locations where they are alone with members of the public).

Note: While bank teller type security structures might provide the greatest level of protection for counter staff, the need for such a level of security needs to be carefully considered given the message that this conveys to members of the public interacting with those staff (and by extension with the organisation). While such arrangements would be quite justified in circumstances where staff are handling money, they are likely to be inappropriate where staff need to build or maintain a level of trust or rapport with the members of the public they deal with.

Security related arrangements or documentation that should be considered include:

- designating security manager for each premises where staff interact with the public
- establishing a security committee to manage security arrangements for the organisation as a whole
- creating a *Restricted Access List* on which all decisions to restrict access or impose alternative service arrangements are recorded
- creating a *Restricted Access and Alternative Service Arrangement Review Schedule* identifying when each decision to restrict access or impose alternative service arrangements needs to be reviewed, and the decision on each review.

Annexure B - Security incident report form

This form is to be completed if there is an incident involving threats, aggressive behaviour and/or violence. An incident includes events such as receiving a threatening phone call, having to terminate an interview because you have been threatened or abused, someone entering our premises without authorisation. [Agencies may well wish to include other categories of security incident in this list].

This form should be forwarded to the [insert titles of security manager and security committee] – either electronically [insert email address] or by hand delivery to [insert title of relevant officer].

Your name		Person's name	
Date of report		Date of incident	
Summary (below)		File Number	
Incident type/category		Select type	
Details of incident			
Details of what action (if any) taken by you			

Annexure C – Tips for responding to threats, aggressive behaviour and violence

1. Recognising danger signals and reviewing risk

Recognise the signs of anger, whether or not the anger is directed at you, and if so whether this is causing you anxiety, distress or fear. Always starting by asking *'Am I in danger?'.* If the answer is *'yes'*, then you should remove yourself from harms way as quickly as possible. In such circumstances, walk through the nearest door into a more secure area, turn and deliver the message that: '*The [insert name of organisation's] policy does not allow me to continue the interview while you are angry or making threats'*. If the circumstances allow, it might be appropriate to convey the message that people becoming emotionally upset in interviews are damaging their interests and also causing distress to our staff. If the threat abates, (ie the persons behaviour de-escalates) then the interview can be recommenced after establishing clear behavioural ground rules.

2. Repeating

Ensure threats are clarified (made overt) and ensure the person takes ownership of the threat by repeating the statement as close to verbatim as possible (eg *'You have just said to me that ...'*), asking if this is what the person meant to say and whether it is in fact a threat to cause harm (eg *'Is that what you meant? Are you threatening me?'*).

3. Reacting

React to all threats by explicitly acknowledging them (whether they are overt or covert, or threats to you, themselves or to others, etc). Always show some reaction to a threat (even if minimal, eg taking a five minute break). However, do not over react to a threat or mirror the threatening language or the threatening behaviour. Continue to show respect even when the person is being rude or threatening.

4. Responding

Ask the person to stop the behaviour (*'Mr ... please stop shouting at me'*) while informing the person of the organisation's protocols for responding to threats – communicating clearly and consistently the repercussions that will flow if the behaviour continues.

5. Redirecting

Redirect or distract the attention of the person with actions or comments that do not reward the behaviour (eg, asking questions about the substantive issues to try to move the person from the 'emotional' state back into a 'cognitive' or thinking state, taking a five minute break, offering a cold drink etc).

6. Refocussing

If the person is able to bring their emotions under control. A question about the facts can refocus a person from their feelings to thinking about the substance of their issue.

7. Raising concerns

If you feel threatened, activate a duress alarm (if available) or leave the room and call for assistance from other staff.

8. Running

If all else fails and you feel an imminent risk of harm – run (or at least move quickly to a safe location).

9. Recording

Always make a 'verbatim' record of all threats and put a copy on the relevant file.

10. Reporting and reviewing responses

Report the matter to your supervisor and the [insert title of the security manager and security committee]. This will facilitate a review of the responses to the threatening behaviour and identification of strategies to manage any future interactions with the person.

Annexure D – Orders to address violence, threats, intimidation and/or stalking

What orders may be available?

Staff might be subjected to threatening, aggressive or violent behaviour in the course of, or as a direct result of, their work. When this occurs immediate action will be taken by [insert name of organisation] to protect their health and safety in accordance with duty of care and workplace health and safety obligations.[1]

There are many different options available to address these types of behaviours, including using the strategies provided in the *Managing Unreasonable Complainant Conduct Practice Manual, 2nd edition*. In limited cases it may also be appropriate to pursue legal options such as an apprehended violence order ('AVO')[2] [or equivalent].

Such an order is a legal order that is issued by the [Local Court under the Crimes *(Domestic and Personal Violence) Act 2007* (NSW), or equivalent in other jurisdictions]. It aims to protect people from personal violence, threats, harassment, intimidation and stalking perpetrated by another person, by placing restrictions on that person.[3]

Such an order may be a legitimate option for managing seriously inappropriate and/or criminal conduct directed at staff in the course of or related to their work. Obtaining an order in appropriate circumstances can ensure a staff member is afforded an appropriate level of protection and can assist [insert name of organisation] to fulfil its common law duty of care and statutory workplace health and safety obligations in the circumstances.

However, the decision to apply for an order is not one that should be made lightly. Such an order can have significant legal and other ramifications for the person the subject of the order, including inadvertently restricting them from accessing essential public or community services. As a result, such an order should only be considered as an option after other reasonably available management strategies have been considered and/or attempted.

In each case where such problems occur the [insert name of organisation] will consider whether to either support the staff member's application for such an order, or to assume responsibility for pursuing such orders in appropriate cases. The [insert name of organisation] might take responsibility for obtaining an order in appropriate circumstances to ensure that:

- careful consideration is given to whether an order is the most appropriate way to deal with inappropriate conduct in a particular case
- the terms of any order issued do not prevent a person from exercising a statutory right or accessing services that are essential to their health and well-being
- people are not inadvertently prevented from accessing services provided by another government agency or non-government service provider located on the same premises
- situations will not occur where multiple staff members obtain such orders in their own right without the organisations prior knowledge, involvement or consideration of the alternatives, and
- management will have an opportunity to explain the reasons for not supporting such an application in a particular case.

---

[1] See *Work Health and Safety Act 2011* (Cth), *Work Safety Act 2008* (ACT), *Work Health and Safety Act 2011* (NSW), *Workplace health and safety Act 2007* (NT). *Workplace Health and Safety Act 1995 (Qld), Occupational Health, Safety and Welfare Act 1986* (SA), *Workplace Health and Safety Act 1995* (TAS), Workplace health and safety Act 2004 (VIC), *Occupational Safety and Health Act 1984* (WA).

[2] AVOs have different names and are regulated under different legislation in each jurisdiction: 'intervention orders' under the Stalking Intervention Orders Act 2008 (Vic); 'protection orders' under the Peace & Good Behaviour Act 1982 (Qld) and the Domestic Violence and Protection Orders Act 2008 (ACT); 'restraining orders' under the Intervention Orders (Prevention of Abuse) Act 2009 (SA), the Restraining Orders Act 1997 (WA), and the Justices Act 1929 (NT); and 'restraint orders' under the Justices Act 1959 (Tas).

[3] Crimes (Domestic and Personal Violence) Act 2007 (NSW), s.10.

When should staff be supported to apply for an order?

To obtain such an order an applicant and/or their representative must show that the applicant has a reasonable and genuine fear of actual or threatened personal violence, intimidation (including harassment[4]), or stalking.[5]

Where a member of staff has such a genuine fear in circumstances where the conduct is a consequence of the work done or services provided by the staff member, then [insert name of organisation] will consider whether to support an application for an appropriate order.

What factors should be considered before supporting a staff to obtain an order?

In addition to considering whether an applicant has a reasonable and genuine fear of harm, the court will also consider:[6]

- the safety and protection of the staff member and other relevant parties
- any hardship that may be caused by making the order, particularly for the staff member, but also for the complainant
- any other relevant issues.

As a result, these factors should be given careful consideration before deciding to support a staff member with an application.

Before agreeing to support an application for an order, the [insert name of organisation] will consider:

- whether the person's inappropriate conduct can be dealt with effectively and appropriately using other management strategies? See *Managing Unreasonable Complainant Conduct Practice Manual, 2nd edition*
- whether the staff member may have contributed in some way to the circumstances that have given rise to need for the application – eg whether the staff member has engaged in misconduct or inappropriate behaviour against the person concerned?
- whether the [insert name of organisation] needs to maintain an on-going relationship with the person concerned or face-to-face contact such that such an order may not be a practicable option?
- whether an order would unfairly restrict the person's ability to gain access to another agency or organisation located on the same premises?
- whether obtaining an order would prevent a person from exercising a statutory right?
- whether continuation of the services provided by the [insert name of organisation] are essential to the person's welfare or wellbeing and/or those of their dependents, if any?
- whether the [insert name of organisation] is the only one, within a reasonable distance, that can provide services to the person concerned – eg if located in a remote location?
- whether such an order would impact on the [insert name of organisation] ability to perform its functions or deliver services to other members of the public/service users?
- what provision, if any, will need to be made to allow contact in emergency situations [where relevant]?
- what the consequences will be for the person concerned and/or their dependents if the order is obtained and/or breached?
- whether an order or proceedings under the [*Inclosed Lands Protection Act 1901 (NSW)* or equivalent] will be the most appropriate legal mechanism to restricting the person concerned from attending the [insert name of organisation] premises? see **Annexure E**.

---

[4] Harassment in a work related context is something more than repeated and/or persistent complaints, phone calls or written correspondence. The persons conduct must be shown to cause a staff member to have a reasonable and genuine fear of harm.

[5] Crimes (Domestic and Personal Violence) Act, s.19.

[6] ibid, s.17.

Annexure E - Restricting access/entry to our premises

Under Australian law owners/occupiers/tenants of private property have the power to grant permission to other persons to enter their premises. This permission may be express or it may be implied in law. Accordingly, members of the public generally have an implied invitation to enter a property that is owned or occupied by a public organisation if that organisation delivers services to the public from those premises – eg face-to-face services.

However, there are times when a person's presence on an organisation's premises may present a significant risk to the safety and security of staff and others, and their access to those premises may need to be withdrawn, for example when a person engages in threatening, aggressive or violent behaviour. In such circumstances action needs to be taken to manage their conduct, which may include withdrawing their right of access to the premises and requiring them to leave and not return. Under these circumstances a person's conduct may also be dealt with under trespass if they either:

- refuse to leave the premises after their access has been withdrawn
- re-enter the premises after their access has been withdrawn without obtaining prior permission.

The [insert title of applicable legislation7] (the Act) empowers owners, occupiers, or persons in charge of 'inclosed lands' [however described in the relevant legislation] to restrict a person from their premises if the person:

- enters their premises without their consent[8]
- remains on their premises after they have been asked to leave[9]
- remains on their premises after being asked to leave and then behaves in an offensive manner[10]
- gives a false name or address when they have been asked to provide this information.[11]

In these circumstances, the Act may be a legitimate option for dealing with a person's conduct particularly in violence is an issue.

However, the decision to use the Act to deal with a person's inappropriate behaviour should not be made lightly. It is an option of last resort that can have significant legal and other ramifications for the person concerned, including restricting them from accessing essential public services. As a result, the Act is an option of last resort after other management strategies have been considered and/or attempted.

What are inclosed lands?

Inclosed lands are defined in the Act as:

[add relevant definition of land covered by the applicable legislation].

This means that any building or office space that is used by an organisation on a permanent, temporary or contract basis to conduct its business is 'inclosed land'.

---

[7] See Inclosed Lands Protection Act 1901 (NSW); Public Order (Protection of Persons and Property) Act 1971 (Cth); Trespass Act 1987 (NT); Land Act 1994 (Qld); Police Act 1892 (WA); Summary Offences Act 1953 (SA); Police Offences Act 1935 (Tas); Summary Offences Act 1966 (Vic); Enclosed Lands Protection Act 1943 (ACT).

[8] Inclosed Lands Protection Act, s 4(1).

[9] ibid.

[10] ibid, s 4A(1).

[11] ibid.

Who within [insert name of organisation] can restrict a person's access to our premises as provided under the Act?

The Act specifies that only owners, occupiers or persons apparently in charge of inclosed lands can restrict a person from their premises. Therefore in the context of [insert name of organisation] it is likely that only the [insert title of CEO] and senior managers will fall within this definition, as well as staff when they are working back late (or come in early) and/or there are neither the [insert title of CEO] or any senior managers present. In these circumstances, such staff may be viewed 'as the person apparently in charge' thereby having an authority to restrict access to those premises (see for example, *Barring Notices/Termination of Licence: Restricting Access to SSWAHS Facilities/Property*).

When might it be appropriate to restrict a person from entering our premises?

It may be appropriate to restrict a person from entering our premises in the following circumstances:

- personal/physical violence including damage to property, firearms offences and other criminal offences such as assault,
- intimidation or harassment such as repeated, uninvited and inappropriate phone calls, hang-up phone calls, text and phone messages, emails, online comments, letters, gifts etc,
- stalking (online or in person),
- threatening or aggressive behaviour or comments in person, over the phone or in writing,
- persistently presenting at our premises while under the influence of drugs or alcohol,
- refusing to leave our premises after legitimately being requested to do so,
- behaving in an offensive manner after being asked to leave our premises.

What factors should be considered before restricting a person from entering our premises?

Before restricting a person's access to our premises in accordance with the Act, the following factors should be taken into consideration:

- Whether the person has been given a verbal, and at the very least a written warning, about their behaviour?
- Whether the person's inappropriate conduct could be dealt with effectively and appropriately using other management strategies? See the *Managing Unreasonable Complainant Conduct Practice Manual, 2nd edition*
- Whether the [insert name of organisation] needs to maintain an on-going relationship or face-to-face contact with the person such that the Act may not be a practicable option?
- Whether using the Act would unfairly restrict the person's ability to access another agency or organisation located on the same premises?
- Whether using the Act would prevent a person from exercising a statutory right?
- Whether the continuation of face-to-face services provided by the [insert name of organisation] is essential for the person's welfare or wellbeing and/or those of their dependents, if any?
- Whether the [insert name of organisation] is the only one, within a reasonable distance, that can provide such face-to-face services to the person concerned – eg if located in a remote location?
- What provision, if any, will need to be made to allow face-to-face contact in emergency situations [where relevant]?
- What the consequences will be for the person and/or their dependents if the warning is breached?
- Whether the or a restraint type order will be the most appropriate legal mechanism to restrict a person's access to our premises in the circumstances?

Annexure F – Special precautions for mail handling

If any mail or its deliverer seems suspicious, do not open it. Check with the recipient as to whether they are expecting a package. Also consider contacting the sender if named and ask if they sent the item. If you are still suspicious, inform your supervisor and the [insert title of security manager]. The following features may attract attention:

- any unexpected item left at the office or lift well
- excess postage having been paid
- the package is unexpectedly heavy
- holes that could have been made by wires
- there are stains or grease marks
- letters are stiff, eg cardboard or metal
- foreign mail, airmail, special delivery items
- restrictive markings such as ‘confidential’ or ‘personal’
- hand written or poorly typed address
- incorrect titles
- titles, but names omitted
- misspelling of common words
- no return address
- excessive securing materials, such as tape or string
- an unusual odour
- audible sounds
- visual distractions such as large stickers or messages on the wrapper, eg ‘fragile’, ‘do not bend’, ‘handle with care’, etc.

Annexure G – Bomb threats

Procedures for staff to respond to a bomb threat

Step	Action
1.	Either refer to the bomb threat checklist on the Intranet, or take comprehensive notes and complete the checklist afterwards.
2.	Let the caller finish their sentences without interruption.
3.	Try to keep the caller talking and try to obtain as much information as possible, including: **when** will the bomb explode **what** the bomb looks like **where** is the bomb located **what** kind of bomb is it **why** was the bomb placed there **details** of the caller (person/organisation responsible) **exact time** of the call and its duration.
4.	**Do not replace the handset even after the caller hangs up.**
5.	Report the threat to your supervisor and the office security advisor immediately.

Procedures for supervisors after a bomb threat is received by a staff member who reports to them

Step	Action
1.	If you believe the bomb threat to be genuine, inform the [insert BCP manager] and [insert title of security manager] and either the Floor Warden or the Chief Warden for the building. This will allow them to take any appropriate action, such as calling the police or evacuating the building.
2.	Ensure the staff member has completed the bomb threat checklist as comprehensively as they can within 24 hours of receiving the telephone call.
3.	Provide the staff member with information about the various support services available to them. See Part 12c *Other remedies* for more information.
4.	Monitor the staff member, particularly when they choose not to use any of the support options provided.
5.	Liaise with the [insert title of security committee] about the possible need for an operational debrief. See **Annexure J** for more information.

Annexure H – Threats with a weapon or hostage situations

Procedures for staff threatened with a weapon or being involved in a hostage situation

Step	Action
1.	Remain calm and try to assess the situation.
2.	If it is safe to do so, activate the duress alarm or call for help.
3.	Follow the aggressor's instructions, but only do what you are told and nothing more. Do not volunteer any information.
4.	Move slowly and avoid eye contact with the aggressor. Advise the aggressor of any movements you have to make which could appear sudden or unexpected, such as opening a drawer. Do not invade the aggressor's space. Keep your hands in view.
5.	Once the threat is over, you will be seen by a senior officer. Once ready you will be asked to complete a Security Incident Report form and email it to the [insert title of security manager and security committee].

Procedures for other staff in the event of a threat with a weapon or a hostage situation

Step	Action
1.	The most senior staff member present, or the [insert title of security manager] should: • override the duress alarm (if it has been activated) and • ring 000 for urgent assistance
2.	Those responding to a duress alarm should attempt to isolate the incident by evacuating the area and stopping others from entering. This would involve standing by the lifts or asking the building management to close off the lifts to the floor.
3.	Follow the aggressor's instructions, but only do what you are told and nothing more. Do not volunteer any information.
4.	The most senior staff member present should: • check that the police have been called • make sure the Floor Warden or the Chief Warden for the building are told what is happening • monitor the situation closely • if it is safe, try to maintain communication with the aggressor until the police arrive.
5.	If the aggressor leaves before the police arrive, the most senior staff member present should provide the police with all relevant information.
6.	Once the threat is over, the supervisor should consult with the [insert titles of office manager and security manager] about the need for advice, counselling or an operational debrief.

Annexure I - debriefing

General Procedures

Step	Action
1.	Report any incident to your supervisor within 24 hours of the incident occurring.
2.	Consider all available options, including debriefing, laying charges, compensation for injury, legal assistance, escorts home, etc.
3.	Discuss debriefing options, including: • informal discussion with colleagues • leaving the office for a walk or a cup of tea • attending an inquiries staff meeting, held every month • an informal discussion with a supervisor • counselling (see contact details below for the Employee Assistance Program) • an operational debrief. An operational debrief will review what took place, and assess what can be done better in the future. This could include changes to safety systems, procedures and training, as well as other issues. The decision to conduct an operational debrief will be made by the [insert title of security manager], in consultation with the supervisors involved. Employee Assistance Program: [number] for traumatic incidents or crisis counselling, call [number].

Debriefing procedures for supervisors when one of your staff is involved in a serious incident

Step	Action
1.	Ensure the staff member involved completes a Security Incident Report form within 24 hours of the incident, and that this is forwarded to the [insert titles of the security manager and security committee].
2.	If the staff member involved is unable to complete the report, ensure that either you or another involved staff member complete the form and email it to the [insert titles of the security manager and security committee].
3.	Make sure the staff member is aware of the support options available to them. These include debriefing, laying charges, counselling, compensation for injury, legal assistance, and escort home, time to recover, etc.
4.	Allow the staff member to discuss the incident if they want to, including what happened, what they did, what they believe they could/should have done and how they feel.
5.	Discuss debriefing options with the staff member.
6.	If necessary, discuss any leave to be taken and re-entry to the workplace. Liaise with Personnel.
7.	Assist in making any necessary arrangements.
8.	Monitor the staff member, particularly when they choose not to use any of the support options provided.
9.	Liaise with the [insert titles of the office manager and security manager] about the need for an operational debrief.

Annexure J - Matters to consider when conducting a risk assessment of public areas

Some of the matters that should be considered when conducting a risk assessment of public contact areas include:

- exits from interview rooms
- exits from reception areas
- exits from conference rooms
- testing the intercom
- counter arrangements – objects on/near counter
- access to work areas
- furniture and layout of interview rooms
- ability of reception staff to monitor interview rooms
- ventilation and thermal control in reception area and interview rooms
- furniture and layout of reception areas
- testing of duress alarms and office response
- review of emergency phone numbers.

Annexure K – Physical security at reception/waiting areas

Key factors impacting on physical security of reception/waiting areas include:

- a stuffy atmosphere or thermal extremes can lead to frayed tempers. If the air conditioning is not working correctly in the reception area or interview rooms, building maintenance should be contacted.
- the physical layout of the reception area can influence a complainant's emotional state. There should be enough seats that are easy to get up from, and enough space to allow ease of movement for wheelchair or pram access.
- throwable objects should be kept to a minimum.
- members of the public are to be excluded from staff work areas except if they are a visitor who has been signed in according to this policy or in exceptional circumstances.
- there should be a door behind the reception desk to allow reception staff to quickly exit to a place of safety. This door should remain closed to deter or prevent a breach of security by a person attempting to access the office by jumping the counter.
- the counter needs to be functional but also provide protection for staff at the initial point of contact with the public. Any object within reach of the public that could be used in an assault (eg stapler, tape dispenser, pot plant) should be kept out of reach.
- there should be a clear glass panel in the wall separating the reception/waiting area and the back office.