Rookwood Necropolis Trust

Disaster Recovery Plan

FEBRUARY 2015

Document title	RNT Disaster Recovery Plan.doc
Prepared	Vicky Critchley/ Ali Nehal
Reviewed	James Evans
Version	Final

Contents

APPENDICES

FIGURES

TABLES

1 Introduction

1.1 Purpose

The purpose of this document is to ensure that the Rookwood Necropolis Trust (RNT) can resume normal operations promptly after an incident. It identifies strategies to secure the Trust's records and IT functionality, and considers other aspects of the Trust's operations including its physical assets and security. The Plan provides key recommendations in respect to general emergency management and handling.

This document is a practical and living document for the RNT Board and staff. It is to be regularly evaluated and updated as circumstances change.

1.2 Defining disaster recovery

In the context of this plan, disaster refers to any event which results in a significant disruption to RNT operations or services and involves reputational, financial or legal/ regulatory liability.

1.3 Aim and objectives

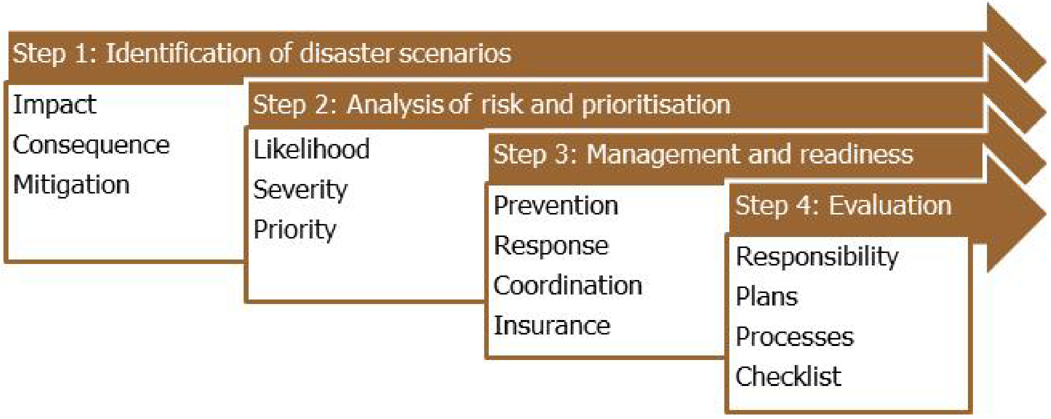
The **aim** of the Disaster Recovery Plan is to assist the RNT to mitigate the damage caused by a major incident and to quickly and efficiently resume normal business.

Key objectives:

- Protect people and property within Rookwood Necropolis
- Proactively manage and minimise the risk of hazards
- Strengthen the capacity of the organisation to respond to and recover from significant incidents
- Encourage coordination and cooperation in planning and management of emergencies.

1.4 Plan process

Figure 1 Process of developing the Disaster Recovery Plan



2 Governance and scope

2.1 Governance

From 1901, following an amendment to the 1867 Necropolis Act, all management of unallocated lands and common infrastructure was under the responsibility of the Joint Committee of Necropolis Trustees. In 2009 the Rookwood Necropolis Act was repealed and the Joint Committee of Necropolis Trustees abolished and replaced by the RNT.

The RNT is managed by a three person board comprising a Ministerially appointed Chair and the CEOs of the Catholic Metropolitan Cemeteries Trust (CMCT) and the Rookwood General Cemeteries Reserve Trust (RGCRT). It continues to be responsible for common lands on behalf of Crown Lands and whole-of-Rookwood functions, although a number of the day-to-day infrastructure maintenance requirements have been devolved to the two Trusts.

The four other management bodies involved in the operation of Rookwood Necropolis are the:

» Catholic Metropolitan Cemeteries Trust (CMCT) – responsible for management of all Catholic lands and infrastructure (including crematoria)

» Rookwood General Cemeteries Reserve Trust (RGCRT)- responsible for all non-denominational and non-Catholic denominational burial lands and associated infrastructure in the Cemetery

» Lessee of the Rookwood Memorial Gardens and Crematorium (Invocare)

» Commonwealth War Graves Commission (CWGC) – manages the Sydney War Cemetery as a lessee of the RGCRT and Commonwealth of Australia licensee for the Garden of Remembrance.

2.2 Scope of the Disaster Recovery Plan

The focus of this Plan is the physical and administrative resources which are under the direct responsibility and management of the RNT. It provides a record of current IT systems and their resilience in the event of a disaster, documenting critical business processes and how they would be impacted by a disaster, and ensuring continued access to policies, plans and procedures. It prioritises Trust functions that are critical to the operation of the Necropolis rather than providing a detailed inventory of all aspects of the Trust's business.

This Disaster Recovery Plan is not intended to be a 'whole-of-cemetery' plan, and primarily addresses only those responsibilities that fall under the RNT. As such it does not specifically address infrastructure or processes under the responsibility of the other two Trusts. It does, however, aim to ensure consistency in processes and procedures across Rookwood, acknowledging that disasters do not necessarily respect administrative boundaries. The Plan therefore seeks to align with and work in tandem with the Disaster Recovery/ Business Continuity Plans of the other two Trusts.

2.3 Rookwood Necropolis Trust assets and responsibilities

The responsibilities of the RNT are underpinned by legislation and/or Ministerial directions or agreement and include:

- Reserve trusts established under the *Crowns Lands Act 1989* with managers appointed by the Minister
- Ministerial Directions made on 25 June 2009, amended and added to in December 2014 (see Appendix B)
- Memorandum of Understanding (MOU) signed 15 August 2012 (see Appendix C).

The RNT own and manage a range of property and infrastructure assets (mainly on Common Property) including the RNT office (located on lot 493), from which Trust operations are based. There are three permanent office employees and one caretaker. The office contains the RNT's paper and digital records.

Also located on lot 493, within Rookwood is the RNT nursery, meeting room and residence. The residential property was previously utilised as the Manager's residence but is now leased out privately.

The Ministerial Directions requires the RNT to:

- Undertake care, control, maintenance and construction of common facilities and infrastructure within the cemetery
- Prepare and implement the Plan of Management for the whole of Rookwood Cemetery.

These Directions provide the RNT with the authority for whole of Rookwood matters and requires the operational trusts (CMCT/ RGCRT) to exercise their functions in alignment with the whole of Rookwood frameworks and plans. The directions are further refined in the Rookwood Necropolis Plan of Management (2014) which is a statutory document signed by the Minister for Primary Industries Katrina Hodgkinson 20th February 2014

Under the MOU, the three Rookwood trusts have agreed to devolve a number of the RNT maintenance and administrative functions to one or both of the operational trusts. There remains however a number of management and operational responsibilities for the RNT.

RNT core responsibilities

- Care and management of RNT assets (Common Property) including primary roads, paths and drains
- Implementation of all components of the Rookwood Plan of Management including associated plans and studies
- Development and implementation of 5 year Capital Works Programme
- Security
- Statistics
- Lodging of Development Applications
- Signage
- Appointment of contractors
- Primary contact for all essential service providers and for the Department of Primary Industries
- Perimeter fencing, gates, setbacks and co-ordination of repairs to fencing and gates.

Out-sourced service provision

IT support is provided by A2K Technologies who manage and monitor the network operations and user support via remote access to the systems and periodic site visits.

Accounting services are provided by the CMCT.

Responsibility for the maintenance of cemetery-wide physical infrastructure is shared between the RNT and the CMCT/ RGCRT.

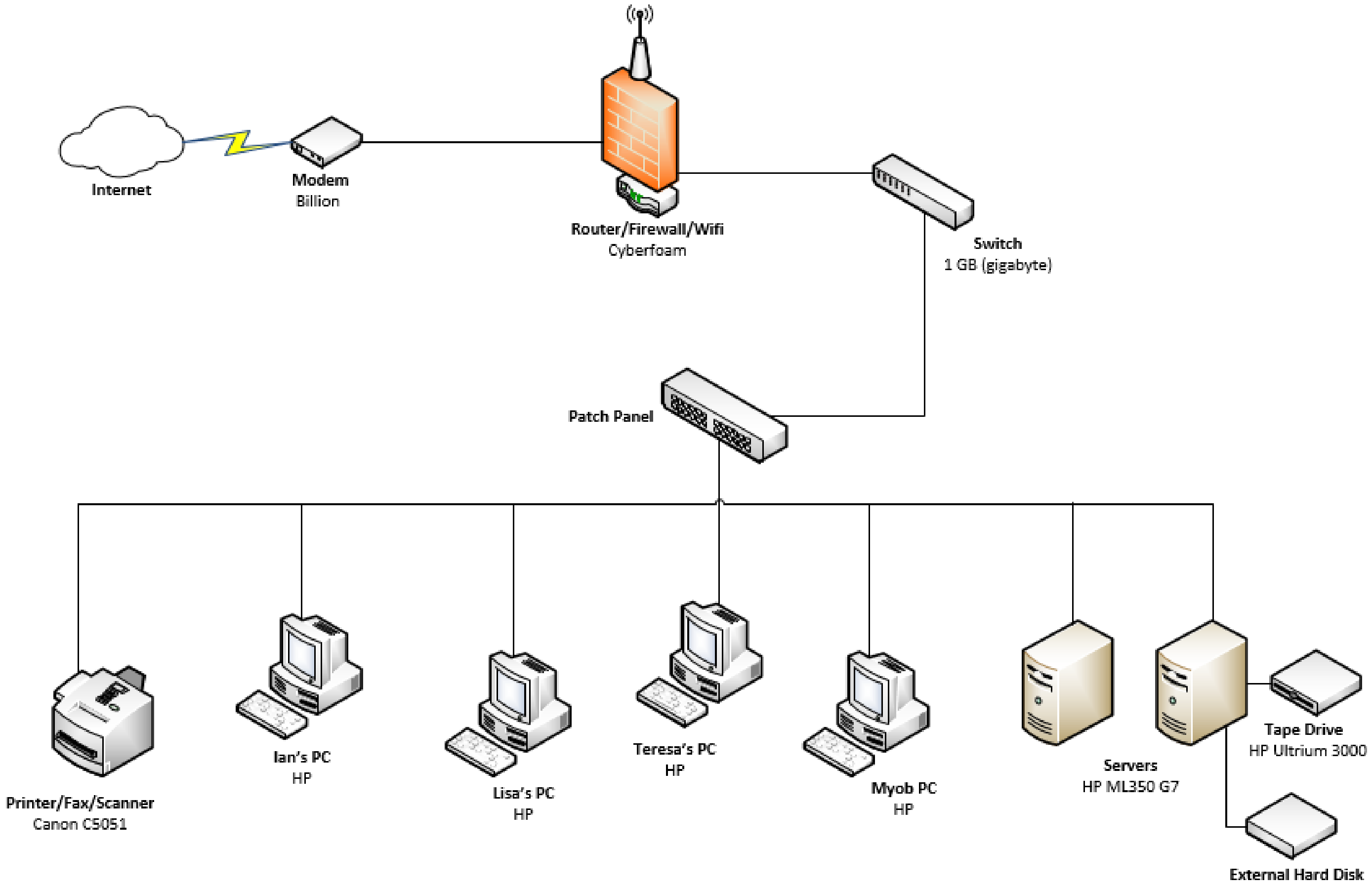
Revenue

RNT revenue is derived from levies paid by the two operational trusts and Invocare (general crematorium lessee) and rental fees collected from Invocare.

Business system and IT infrastructure

The Rookwood Necropolis Trust's local area network comprises of two servers running Windows Small Business Server 2011 and five personal computers running Windows 7. All this sits behind a router and firewall and is connected to a Gigabit switch located in the server cabinet. The cabinet also houses an external tape drive and an external hard disk drive for backup purposes The RNT is connected to the internet via an ADSL modem. Users can access their emails using Microsoft Outlook from their PCs in the office and remotely from their homes or outside using Outlook Web Access.

Figure 2 RNT local area network



3 Disaster scenarios

There are two broad categories of disasters that have the potential to disrupt business and service operations of the RNT; natural and man-made. A natural hazard is a naturally occurring geological or climatic event that has the potential to detrimentally impact the surrounding environment, human assets and life. Man-made impacts are disruptions that are caused by the planned or accidental actions of a human agent or involve software or hardware malfunctions.

Listed below are those disasters which are most likely to directly impact the functions of the RNT. The likely scale and range of impacts of the disaster on the RNT are also summarised.

3.1 Natural hazards

There are a number of natural hazards which could potentially cause extreme damage to the Cemetery however many (such as earthquakes or tornados) rarely occur in Australia. Natural hazards that are relatively common in the Sydney region are extreme storm events, droughts and bushfires.

CSIRO and the Bureau of Meteorology (BoM) have advised that global warming will likely result in increased severe weather events in the Sydney metropolitan region including more flooding events from less frequent but more intense rainfall events (Henessey et al 2004). While it is too early to state conclusively that recent extreme weather events are a consequence of climate change, there is mounting evidence that these are occurring more commonly in the Sydney region.

Severe storm events

The main impacts of severe thunderstorms in the Sydney metropolitan region are localised flooding, lightning strikes and wind gusts. Over 100 severe storms affect New South Wales each year, they have a distinct seasonal and daily pattern, occurring largely in the summer months (from November to February) and spiking in frequency in the afternoon (between 2-6pm).

The costliest natural disaster in Australian insurance history occurred in April 1999 when a supercell storm caused a swathe of damage along Sydney's inner west and eastern coastal suburbs, with hails the size of tennis balls (>9cm) accompanied by torrential rain and high winds. The damages reached an estimated A$2.3 billion (Schuster et al 2005). On average, there are over 8 reports of large hail (>2cm) in the Sydney metropolitan region annually (NSW BoM – accessed 15/01/2015).

Table 1 Severe Storm Disaster Scenario

Impact	Consequence	Notes
Localised **flooding** of roads and grounds	Temporary disruption of traffic and cemetery services Failure of drainage and sewerage infrastructure	A recent report on the cemetery's water infrastructure stated that "flooding on site does not impact on the cemetery's operations and drains quickly" (Engeny 2014).

Impact	Consequence	Notes
Regional **blackout**	Loss of telecommunication and information services All administration services suspended till electricity restored.	While functions would be disrupted by power loss it is unlikely to cause any long-term or major impact on RNT operations
Direct **lightning** strike on the office	Local power surge causing damage to telecommunication and information devices Fire ignited and either partial or complete loss of structure, equipment and documents (hard/soft copy)	Under existing legislation, telecommunication and electricity service companies are required to install direct strike protection equipment.
Direct **lightning** strike in the grounds	Damage to physical infrastructure Personal injury	There are general WHS procedures for all contractors but these do not specifically relate to natural hazards.
Major **wind** gusts	Significant damage to office - either partial or complete loss of structure, equipment and documents (hard/soft copy) Personal injury caused by flying debris Loss of major vegetation and damage to physical infrastructure (e.g. fences, signs and sheds) Obstruction of road network (vegetation/ debris across roads and footpaths)	There are no historical records of wind having caused major damage to RNT physical assets.
Large **hail** event	Significant damage to buildings and physical infrastructure Disruption of travel (hail across road and pedestrian infrastructure) Personal injury	There is no protection for RNT vehicles during a hail storm – however insurance should cover any physical damage.
Post-storm - Falling or damaged **trees/ branches**	Physical infrastructure damage Personal injury	An arborist is employed to check for dangerous tree or limbs post major storms.

Fire

“The majority of more intense fire seasons have occurred since the late 1990s, with seasons starting earlier and finishing later.” (C. Lucas et al, 2007). Under present projections the incidence of catastrophic fire days would nearly double by 2020 along Australia’s eastern seaboard. (K. Hennessy et al, 2008). In urbanised areas, human factors (accidental or deliberate) are a common vector of bushfires (Geoscience Australia – accessed 15/01/2014).

Bushfires have occurred within the cemetery, but with less frequency as the majority of the 286 hectare site is landscaped with substantial lawns and scattered mature trees. The remaining pockets of environmentally significant indigenous bushland in Rookwood are protected as Vegetation Conservation Areas.

Table 2 Bushfire Disaster Scenario

Impact	Consequence	Notes
Fire damage to grounds	Damage to physical infrastructure and vegetation Personal injury	RNT has developed a Bushfire Management Plan. Vegetation Conservation Areas are no longer subject to hazard control however they are fenced and isolated.
Fire damage to administration building	Either partial or complete loss of structure, equipment and documents (hard/soft copy) Personal injury	There are smoke detectors in the administration building An evacuation plan has been prepared.

Droughts and dust storms

Australia is the driest inhabited content in the world and has common periods of drought. These are usually associated with the El Nino – Southern Oscillation. It is likely that climate change will lead to more frequent dry periods (and even dust storms) in Sydney (Hennessy et al 2007).

Table 3 Drought and dust storm disaster scenario

Impact	Consequence	Notes
High level **water restrictions**	Browning of lawns and vegetation Loss of trees	RNT has a permit to use water for irrigation during an imposed water restriction period.
Major **dust storm** – loss of visibility	Cessation of external activities Disruption of travel Damage to mechanical equipment Respiratory health impacts	While functions would be disrupted a dust storm is unlikely to cause any long-term or major impact on RNT operations

3.2 Human impacts and technical failure

Information technology

This refers to any loss of business continuity due to damage or incident of a technical nature, relating to its administrative functions. Damage to the RNT's hardware or software has the potential to impact any or all of the following:

- Communications – telephone, facsimile, email and internet
- Digital records and accounts
- Computer-based administrative functions.

In order to address loss of partial or systematic data the RNT has in place an existing data back-up regime:

- Nightly full backup of all data including Exchange server mailboxes and public folders tape using Symantec Backup Exec
- RNT is using a tape drive with 22 tapes (10 tapes on a two weeks rotation and 12 tapes for monthly backups).

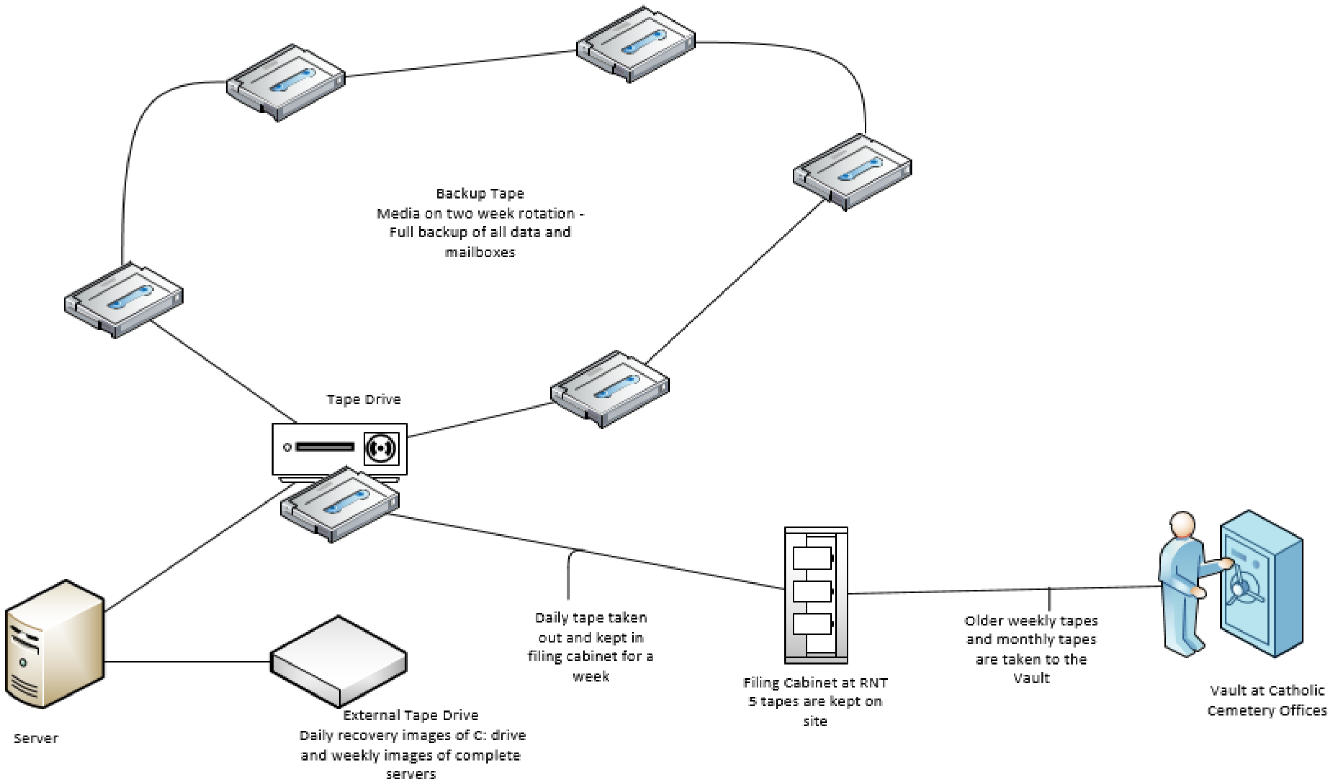
- Five tapes for each weekday are kept on site
- The rest of the tapes including the monthly backup tapes are kept offsite in a vault in the Catholic mausoleum.
- A Symantec System Recovery creates an image of the C: drive to an external hard drive during the week. In addition, a complete image of the servers including operating system and data is created every weekend and saved on to an external hard drive.

IT support is outsourced to a company called A2K Technologies.

Table 4 Information technology disaster scenarios

Impact	Consequence	Notes
Hardware equipment failure	Loss of data	There is both on-site and off-site back-up of data as well as additional hardware equipment.
External system outages (including blackout)	Loss of telecommunication and/ or information services All administration services suspended till services restored.	Mobile phones provide communication access and can provide internet service in an emergency.
Activation of a **virus or Trojan horse**	Loss of data or data corruption Data and website security compromise	Anti-virus software is installed and updated daily.
Operational error	Loss of data	On-site and off-site back-up of data.

Figure 3 RNT backup process



Criminal activity

Due to the open nature of Rookwood Cemetery and the ease of access (gates are open from dawn to dusk every day) petty theft is a fairly common occurrence. Official opening hours for Rookwood are:

Summer Time (01 Oct – 31 Mar) 6.00am – 9pm.

Winter Time (1 Apr – 30 Sep) 6.00am – 7pm)

Of greater concern to the RNT is the potential for a break-in of the administration centre and vandalism of property. There have been a number of high-profile funerals (involving either bike groups or criminal elements) which have resulted in a high police presence. In a recent incident, over 70 Russian, Serbian and non-denominational graves were vandalised during a late night break-in, underlining the difficulty of securing a 286 hectare site. Despite this incident, the likelihood of Rookwood Cemetery being a primary target for a significant terrorist attack is unlikely.

Table 5 Criminal activity disaster scenarios

Impact	Consequence	Notes
Burglary	Loss of IT equipment (including digital records and data security) Loss of operational equipment including plants	There has not been a major burglary of the RNT office.
Vandalism	Damage to property and operational equipment	The RNT utilises CCTV cameras at both entry and exit gates.
Bomb threat or **hostage** situation	Cemetery lock down Personal injury	See above.

Misadventure

Misadventure refers to a range of accidents that may occur within Rookwood Cemetery as part of its everyday operations, it includes car accidents, disability or death of a key staff member and accidental damage to facilities and infrastructure. As a small organisation the impact of the loss of a key staff member would cause much greater disruption than for a major company.

The key concern for RNT is to maintain the flow of traffic on the primary road system and ingress/egress through the two entrance gates. The Trust relies on the NSW Police to enforce speed and traffic regulations within the cemetery. Despite occasional high traffic volumes from commuter and visitor traffic, most vehicles within Rookwood are travelling at low speed and serious accidents rarely occur.

Although unlikely, a fire in the administration building could cause significant damage, from either the fire or associated water damage, if emergency services were required. The most significant loss, aside from the potential for personal injury, would be damage to cemetery records that have been neither digitised nor archived.

Table 6 Misadventure disaster scenarios

Impact	Consequence	Notes

Impact	Consequence	Notes
Disability or death of key staff member	Loss of management oversight and institutional knowledge	The RNT employs a number of ancillary consultants who are highly knowledgeable about the operations of the cemetery and would be available to assist as needed.
Major **car or pedestrian accident** on the primary road network	Partial or complete closure of road system or entrance Personal injury	NSW Police occasionally police traffic and parking within the Cemetery.
Damage to major service infrastructure (gas line/ water pipe or electrical cable)	Evacuation of area Localised flooding Power outage	Signage and information is provided regarding the placement of underground services.
Electrical **fire**	Either partial or complete loss of structure, equipment and documents (hard/soft copy) Personal injury	There are smoke detectors in the administration building An evacuation plan has been prepared.
Infectious disease epidemic (such as pandemic influenza/ Ebola)	Perceived or real personal safety Restrictions on public access Strain on cemetery resources	RNT is not directly involved in burial procedures but as the overall cemetery Manager may be involved in the response particularly community education and public control.

4 Risk assessment

A risk assessment of potential disaster scenarios has been undertaken to highlight those incidents which require most attention and consideration by the RNT. This assessment in no way replaces specific project and operational risk assessment which should be undertaken as a standard approach to RNT activities (as described in the Rookwood Necropolis Trust Risk Management Plan).

4.1 Methodology

The first step in risk assessment is to determine the level of management response required by the RNT based on the impact of the incident and the likelihood of it occurring.

Disaster scenarios have been ranked in respect to their priority for action based reviewing incidents according to the following tables.

Step 1: Identify the severity of each incident according to the following categories. The rating has been based on the highest potential consequence of any one category.

Table 7 Rating of severity based on the potential consequences of the incident

Rating	Description	Safety	Assets	Services	Reputation	Liability
1	Minor	Minor injury – first aid or minimal medical treatment	Minor damage (<$5,000)	Minor disruption (<24 hrs)	Slight impact	Potential minor regulatory fines
2	Moderate	Serious injury – hospitalisation	Significant damage (<$50,000)	Significant disruption (< 1 month)	Local impact - local media/ visitor attention	Potential for significant legal/ regulatory fines
3	Major	Long-term illness or fatality	Major damage (<$500,000)	Major disruption (< 1 year)	National impact – national media/ industry attention	Potential for major legal/ regulatory fines
4	Catastrophic	Multiple fatalities	Extensive damage/ loss of property (>$500,000)	Extensive disruption (> 1 year)	International impact – international media attention	Potential for criminal liability

Step 2: Rate the likelihood of the incident occurring based on the following categories.

These ratings range from ‘rare’ (have never happened and are unlikely to take place) to ‘likely’ (have happened in the past and are highly likely to occur again).

Table 8 Rating of likelihood of the event occurring

Rating	Level
1	Rare
2	Unlikely
3	Possible
4	Likely

Step 3: Identify a management risk level based on the potential severity and the likelihood of an event occurring

This uses cross-tabulation to identify which incidents present the highest management priority for the RNT.

Table 9 Management risk level rating

Severity Likelihood	1	2	3	4
1	🟩	🟩	🟩	🟨
2	🟩	🟩	🟨	🟧
3	🟩	🟨	🟧	🟥
4	🟨	🟧	🟥	🟥

Table 10 General management response advised for the risk level

Rating	Impact	Response
1	Minimal risk to RNT operations or services	No additional formal management response required
2	Moderate risk to RNT operations or services	Review mitigation measures – no major steps required
3	Significant risk to RNT operations or services	Review and update mitigation measures - high response priority
4	Severe risk to RNT operations or services	Review and update of mitigation measures – regular reporting to the Board of vulnerability.

4.2 Priority matrix

Each of the disaster scenarios was given a priority rating based on the likelihood of the incident occurring and the potential severity of the consequence for the RNT.

Table 11 Natural hazards priority rating

Impact	Likelihood	Severity	Priority
Localised flooding of roads and grounds	2 (unlikely)	1 (services)	🟩
Regional blackout	3 (possible)	1(services)	🟩
Direct lightning strike on the office	1 (rare)	3 (services/ assets)	🟩
Direct lightning strike in the grounds	2 (unlikely)	2 (assets/ safety)	🟨
Major wind gusts	4 (likely)	3 (services/ assets/ safety)	🟥
Large hail event	3 (possible)	2 (services/ assets)	🟨
Bushfire damage to administration building	1 (rare)	3 (services/ assets)	🟩
Bushfire damage to grounds	3 (possible)	2 (services/ assets)	🟨
High level water restrictions	4 (likely)	1 (assets/ reputation)	🟨
Major dust storm – loss of visibility	2 (unlikely)	1 (service/ assets)	🟩

Table 12 Man-made hazards priority rating

Impact	Likelihood	Severity	Priority
Burglary	3 (possible)	1 (assets)	🟩
Vandalism	3 (possible)	2 (assets/ reputation)	🟨
Bomb threat or hostage situation	1 (rare)	4 (reputation/ safety)	🟨
Disability or death of key staff member	2 (unlikely)	4 (services)	🟧
Major car or pedestrian accident	2 (unlikely)	2 (services/ safety)	🟩
Damage to major service infrastructure	4 (likely)	2 (assets/ services)	🟧
Electrical fire - damage to administration building	1 (rare)	4 (assets/ services)	🟨
Infectious disease epidemic	1 (rare)	2 (services/ safety/ reputation)	🟩
Hardware equipment failure	3 (possible)	1 (assets/ services)	🟩
External system outages	4 (likely)	1 (services)	🟨

Impact	Likelihood	Severity	Priority
Activation of a virus or trojan horse	4 (likely)	2 (services/ assets/ reputation)	🟧
Operational error	4 (likely)	1 (services)	🟨

5 Readiness and response

Listed below are the management readiness and responses designed to address the key scenarios identified in sections 3 and 4.2. The focus of this section is those issues which are likely to significantly impact the operations of the RNT.

5.1 Readiness measures

Listed below are basic actions to mitigate the impact of any natural or man-made disaster. A number of these actions have already been undertaken by the RNT as referenced in the right hand 'status column.

Table 13 Natural disaster preparation

Actions	RNT Responsibility	Priority	Status
Prepare an emergency kit (including battery operated torches/ radio/ first aid kit/ emergency contacts) for use in a natural disaster.	Office administrator	High	**Review and update**
Prepare an emergency evacuation plan (which identifies when staff should 'shelter in place', evacuate to an alternative building within the Cemetery or to a site external to Rookwood as well as key document/items within the office to be protected).	Office administrator	High	**In place**
Identify critical business documentation and develop steps for safe storage and/or removal if required	Office administrator	High	**In place**
Review adequacy of RNT insurance in relation to a natural disaster. Major reviews should be conducted every five years.	Board/CEO	High	**Review and update** **Last review:**
Listen to forecasted weather warnings and obtain advice as required from SES or RFS personnel regarding the duration and severity of the natural event (e.g. severe storm, bushfire or heat wave). Based on reports and advice from the appropriate authorities determine whether » outdoor work activities, external meetings or other commitments should be rescheduled » non-essential staff should be asked to either stay or return to their home » Rookwood Cemetery should be temporarily closed.	CEO/Office administrator	High	**In place**

Actions	RNT Responsibility	Priority	Status
An alternative emergency shelter and office space should be identified for either short-term or long-term use during and following a major natural disaster.	Board/CEO	Medium	**In place**
Undertake a regular inspection of RNT drains, canals and sewage systems to ensure that they are well-maintained and free of debris. Inspections to be conducted monthly during peak storm periods (November – February) and/or after severe storm events.	CEO	Medium	**In place**
Ensure regular maintenance of the RNT office roof and gutters to prevent possible leakage during a severe storm and to reduce bushfire threat. Gutters should be cleaned monthly during peak storm periods (November – February) and/or after severe wind events. Roofs should be inspected every 3-5 years.	CEO	Medium	**In place**
Make an itemised list of any large items (such as shelters, fencing or signage) that may pose a hazard if there is a severe wind event. Identify a risk management process to secure or safely store any large moveable objects if a major wind event is forecast.	Office administrator	Medium	**To implement**
Undertake a regular safety audit of major trees adjacent to RNT pathways and significant infrastructure/ assets. Major trees should be inspected annually prior to the peak storm season (i.e. in October) and following severe storm events.	CEO	Medium/ Low	**Review and update**
Review hazard management and fuel reduction needs for Vegetation Conservation zones from both an ecological and asset protection perspective.	CEO	Medium/Lo w	**In place**
Undertake periodic testing of external fire hydrants and assess whether there are adequate resources to manage a major bushfire event.	CEO	Low	**In place**

Table 14 Mitigating misadventure and systems failure

Actions	RNT Responsibility	Priority	Status
Install and regularly upgrade antivirus programs.	A2K Technologies	High	**In place**
Prepare and inform staff of protocols for IT security such as receipt of unknown emails, installation of external software and movement of files between personal and office equipment.	Office Administrator/ A2K Technologies	High	**In place**
Regularly update software security patches and enable automatic installation of software updates.	A2K Technologies	High	**In place**
Ensure backup schedules are maintained and allow for full operational recovery.	A2K Technologies	High	**In place**
Purchase 'key person' insurance to cover the disability or death of the CEO.	Board	High	**In progress**
Develop a succession plan which covers the planned succession of the CEO and contingencies for emergency replacement of RNT staff.	CEO	High	**To implement**
Review and refine mapping of major service infrastructure within the cemetery.	CEO/Office Administrator	High	**Review and update**
Set up a work plan to scan and archive contemporary and historical paper records.	Office Administrator	High	**In place**
Purchase redundant and ancillary equipment to allow for continued business operations following hardware or systems failure (E.g.: back-up server, PC and internet dongle, spare laptop battery).	Office Administration	Medium	**In place**
Ensure office laptop and battery are fully charged	Office Administration	Medium	**In place**
Develop a records management strategy that outlines the responsibility of all staff regarding the management of information	Office Administration	Medium	**In place**
Prepare a records register that identifies what, where and how information is stored regardless of format and provides a process to support document security (i.e. scanning, storage and archiving)	Office Administration	Medium	**Review and update**
Monitor alert levels and security warnings by the Federal and State Government. Take particular note during major events at Rookwood and high profile/ high-risk funerals.	CEO/Office Administrator	Medium	**To implement**
Undertake regular maintenance of security systems including review of fences, gates and	CEO	Medium	**In place**

Actions	RNT Responsibility	Priority	Status
CTV equipment.			
Review procedures and signage to inform contractors of service infrastructure prior to construction works.	CEO/Office Administrator	Medium	**In place**
Identify an alternative office space, including essential IT equipment within Rookwood for either short-term or long-term use in case of disruption of office utility.	CEO/ Office Administration	Medium	**In place**
Undertake periodic testing of smoke detectors and fire drills for the RNT office. Review RNT office fire equipment, including purchase of a portable fire extinguisher. Note that, by law, all extinguishers must be inspected and serviced every 6 months by a properly qualified person.	Office Administrator	Medium/ Low	**In place**

5.2 Response and recovery

Identified below are the measures to ameliorate a number of the more serious consequences of either natural or man-made disasters.

Table 15 Disaster recovery plan

Consequence	Response and recovery measures	Responsibility	Key contacts
Either partial or complete loss of office structure, equipment and documents (hard/soft copy).	General: » Talk to emergency services to find out if it is safe to visit the premises » List and photograph any damage to building, assets or documents If office is still usable: » Cordon off area that has been damaged » Contact appropriate providers (see above) if any electrical/ telecommunication infrastructure has been affected » Contact insurers to determine whether there are any claims that need to be initiated » List steps needed to recover the damage and work out who and timing for completion, If office is not usable: » Contact Board and organise alternative office space » List the key contacts to assist in maintaining business operations (i.e. accountant/ financial advisor) » Salvage any equipment, records or assets that can be utilised or need to be stored » Contact insurers to initiate a claim » Provide information and signage to notify of the changed office circumstances.	Office Administrator/ CEO Office Administrator/ CEO/ Board	Energy – Ausgrid: 131 388 Telephone – Telstra: 132 203 Internet – Telstra: 133 933 Insurer – GIO: 131 010 or QBE: 133 723

Consequence	Response and recovery measures	Responsibility	Key contacts
Damage to external physical infrastructure and vegetation	» Contact appropriate Trust Operations Manager » Contact arborist to inspect damaged trees » If service related – contact appropriate service provider » Assess damage and take photographs if required for an insurance claim » Secure area and put in place detour provisions, if required » Inspect assets following maintenance and repair.	CEO	CMCT Operations Manager – John Richardson 0417 062 322 RGCRT Operations Manager - Mark Bundy 0418 414 457 Water - Sydney Water:132 090 Energy – Ausgrid: 131 388 Gas – Jemena: 131 909 Insurer – GIO: 131 010 and/or Allianz: 131013
Obstruction of road network	» Contact appropriate Trust Operations Manager » Erect signs and put in place detour provision » Close gate as required » If there is a vehicle accident, notify the Police.	CEO	CMCT Operations Manager – John Richardson 0417 062 322 RGCRT Operations Manager - Mark Bundy 0418 414 457 Car accidents - Police Assistance Line: 131 444
Personal/ public injury	» Assess situation and administer first aid if possible - call an ambulance as required. » Take down notes about the incident and if possible photograph the cause of the injury » Fill out incident proforma » Notify insurers and RNT lawyers	Office Administrator	Insurer – GIO: 131 010 or QBE: 133 723 Lawyers – Houston Dearn O'Connor: (02) 9744 9247
Temporary loss of electricity, telecommunication and information services	» Contact appropriate provider to identify likely cause and length of issue » Switch over to mobile phones » Switch over to laptop with wireless internet dongle » If power is likely to be off for more than 24 hours consider utilising an alternative (or home) office space.	Office Administrator	Energy – Ausgrid: 131 388 Telephone – Telstra: 132 203 Internet – Telstra: 133 933

Consequence	Response and recovery measures	Responsibility	Key contacts
Data loss[1]	» Verify cause of data loss » If data loss caused by equipment failure – use redundant equipment (computer/ server) » Mount and run backup tape on tape drive » Upon verification of restored data, dismount and eject tape and replace tape back into storage onsite/offsite » Fix or replace equipment as required.	Office Administrator	IT support - A2K Technologies: 0404 831 825
Data corruption or security compromise	» Verify extent of damage and cause of virus activation (i.e. identify how long the virus has been in the system and the extent of infection) » Disconnect PC from network if the virus is isolated » Run anti spyware/malware software on PC/s and servers as required » Scan until the computer/s are completely clean » Restore data/software from clean backup.	Office Administration	IT support - A2K Technologies: 0404 831 825
Failure of security system	» Verify extent and cause of security system outage » Verify security data has been backed up and is safe » Contact guard agencies to source on-site guards » Define guard duties and brief guards on duties » Contact supplier to get a replacement system - units/cameras/sensors as required. » Test and install new security system.	CEO	Security patrols - SNP Security: (02) 9667 5200
Extensive damage to Cemetery	» Contact local Police	CEO	Police – Flemington Local

[1] Data files can be recovered from tapes for a maximum retention period of two weeks. Any recovery beyond the last 14 days is available on monthly tapes for up to a year. If there is a complete crash of the server, data can be restored using the recovery backups saved on the external hard drive given the server is fixed or replaced.

Consequence	Response and recovery measures	Responsibility	Key contacts
assets (vandalism)	» Assess damage and take photographs if required for an insurance claim » Arrange a meeting with other Trust managers to discuss and review security arrangements.		Area Command (LAC): 02 9646 8699 CEO RNT - Ian Mc Intosh: 0417 449 159
Cemetery lock down (Bomb threat/ hostage situation)	» If receiving a bomb threat by phone – keep calm and keep talking. Try and ascertain: > Who is talking > Location of Bomb > Time set to explode » Contact the police and security » Inform key contacts in the Cemetery » Be prepared to evacuate » Be observant and make notes as soon as possible to assist authorities with their investigation » Identify counselling services for affected staff as required.	Board/ CEO	Emergency services – 000 Department of Primary Industries (02) 8574 6200 CEO RNT - Ian Mc Intosh: 0417 449 159
Loss of management oversight and institutional knowledge	» Contact Board and financial advisors » Organise for temporary replacement of staff as required » Contact insurers	Office administrator/ CEO/ Board	Insurer - GIO: 131 010 CMCT- CFO: 02 8713 5700 RGCRT - CFO: 02 9746 2177
Notification of infection disease	» Liaise with the Department of Health » Organise regular updates with other Trust Managers		NSW Health – Local Public Health Officer: 02 9845 5555

5.3 Emergency information

Prior and during an emergency it is essential that the best advice can be received and that appropriate authorities are notified to support response and recovery operations.

Table 16 Emergency services and information

General emergency	Police and ambulance	000
Severe storm	State Emergency Services Bureau of Meteorology	132 500 / www.ses.nsw.gov.au www.bom.gov.au/nsw/forecasts/sydney.shtml
Bushfire information	NSW Rural Fire Service:	1800 679 737 / www.rfs.gov.au
Fire/ misadventure	Fire and Rescue NSW	000/ www.fire.nsw.gov.au
Criminal activity	Local Police	Flemington Local Area Command (LAC): 02 9646 8699
Terrorism threat	Australian National Security	Hotline: 1800 1234 00 www.nationalsecurity.gov.au/Securityandyourcommunity/Pages/NationalTerrorismPublicAlertSystem.aspx
General broadcasting	ABC news and radio	www.abc.net.au/news/emergency/state/nsw/ 702 Local radio

6 Summary of recommendations

Listed below are a number of recommendations to support the identified aim of assisting the RNT to mitigate the damage caused by a major incident and to quickly and efficiently resume normal business.

Risk management

1. RNT should review its Risk Management Plan to incorporate procedures to mitigate the impacts of a severe storm, in particular severe wind gusts on the cemetery's physical infrastructure.
2. Consideration should be given to undertaking a whole-of-cemetery review of drainage assets and other critical infrastructure to determine capacity to meet predicted climate events as a consequence of future global warming.
3. Provide a template (see Appendix F) to encourage the other Trusts and Invocare to advise the RNT when a high profile or controversial funeral is to be conducted.
4. Fund a program to scan and archive contemporary and historical paper records.

Information technology

5. RNT should purchase 4G wireless internet sticks (dongles) from Telstra on a data plan as well as at least one laptop for the office. RNT can use the dongle and laptop whenever it loses power or connectivity to the internet because of router or wireless device or ADSL link failures. In order to support extended operational use during a major blackout, RNT could purchase a universal laptop battery that comes with a variety of 'tips' to suit most computer brands. The battery should be stored charged up, and can then be connected to the laptop's power socket when the internal battery runs low. The external battery charges the internal battery or, if the internal battery is removed, powers the laptop directly.
6. RNT should purchase an additional external hard drive to alternate with the existing hard drive that is located onsite for server backups. The hard drives, on a rotational basis, should be removed offsite to the vault at the Catholic cemetery along with the weekly tapes. This is a highly cost-effective method to support complete server recovery and minimise downtime, in the event of a total site disaster.
7. RNT should replace the FileMaker document management system. It should investigate a system called SOHODOX. SOHODOX is a Windows based document management software where documents are stored and organised. It creates a centralised, searchable, multiuser database of all of the documents. It works with any TWAIN-compatible scanner (such as RNT's existing copier) and saves documents in a wide range of formats, including PDF and TIFF. FileMaker files can be imported into SOHODOXby using the 'export data' tab to turn tables into CSV files. The data from the CSV files can then be imported into SOHODOX as Document Types.
8. Once the Lacie hard disk drives and Sony 3 DAT tapes are able to be accessed (see below for details) the RNT should preserve the data in an alternative form as the tape media and tape drive are now obsolete. The tape contents can be transferred over to a folder on the hard drive, then either copied onto standard DVD or Blu-ray discs and archived offsite or saved onto the RNT document management system.

In order to access the old data currently residing on the Lacie hard disk drives, RNT needs a Mac computer to access data from the old Lacie disk drives and the following accessories:

» Firewire 800 to Firewire 800 (9-to-9 pin) cable and a Firewire 800 equipped (9-pin) Mac running OS 10.2 or greater

» Firewire 400 to Firewire 400 (6-to-6 pin) cable and a Firewire equipped (6-pin) Mac running OS 9.x or 10.x

» Hi-Speed USB 2.0 cable and a Mac running 10.2 or greater or USB 1.1 cable

» USB 1.1 cable and a Mac running OS 9.x or 10.x

In order to read the old data from the Sony 3 DAT tapes, RNT needs a tape drive, such as the Sony SDT 10000, along with Backup Exec software version 9 or 10 running on a server. The tape drive needs to be attached to the server with a SCSI cable and detected by the backup software. A SCSI cable is also needed to connect the tape drive to the SCSI port on the server and a SCSI terminator on the tape drive.

7 Evaluation and communication

7.1 Evaluating the plan

The intent is for this Plan to be a practical and living document for the RNT Board and staff. Once the document has been signed off by the Board it is recommended that the following review schedule be adopted.

1. Annually with an evaluation of the status of the risk assessment, the readiness and response measures and recommendations provided to the CEO and Board. All key stakeholder and support contacts should also be checked and updated as required (see Appendix E)
2. Following a major incident, the corresponding mitigation and response measures should be reassessed and risk levels adjusted if required. Any intensification of the incident priority should be reflected in management processes such as the Risk Management Plan.
3. Risk levels and priority ranking of critical incidents should also be reviewed following advice from appropriate authorities.

7.2 Plan communication and implementation

An overview of the role and responsibility of staff for communication and implementation of the Plan has been set out below.

Table 17 RNT staff Disaster Plan roles and responsibilities

Who	Contact	Role
RNT Board		Signs off on and oversees implementation of the Disaster Recovery Plan. Provides recommendations regarding the need for evaluation and review.
RNT CEO	Ian McIntosh 02 9746 8433	Reports to the Board regarding implementation of the Plan. Communication of the plan to external stakeholders including other trust bodies and emergency services.
Office Administrator	Lisa Elliot 02 9746 8433	Coordinates implementation of recommendations and provides regular reviews of the plan, response and readiness status and checklist. Communicates with internal staff to ensure knowledge of the plan and key mitigation and response measures.

Appendices

A Bibliography

Engeny Water Management (2014) *Surface Water Report Rookwood Necropolis Landscape Masterplan*

Hennessy, K., Fawcett, R., Kirono,D., Mpelasoka, F., Jones, D., Bathols, J. (2008). A*n assessment of the impact of climate change on the nature and frequency of exceptional climatic events.* Canberra: Bureau of Meteorology/CSIRO.

Hennessy, K., B. Fitzharris, B.C. Bates, N. Harvey, S.M. Howden, L. Hughes, J. Salinger, and R. Warrick. (2007). Australia and New Zealand. In *Climate change 2007: Impacts, adaptation and vulnerability.* Contribution of Working Group II to the Fourth Assessment Report of the Intergovernmental Panel on Climate Change. Edited by M.L. Parry, O.F. Canziani, J.P. Palutikof, P.J. van der Lindenm, and C.E. Hanson. Cambridge University Press, pp. 507-540

Hennessy, K., Page, C., McInnes, K., Jones, R., Bathols, J., Collins, D., and Jones, D. (2004). *Climate Change in New South Wales. Part 2. Projected Changes in Climate Extremes.* Consultancy report for the New South Wales Greenhouse Office by CSIRO and the Australian Bureau of Meteorology.

Lucas, C, Hennessey, K, Mills, GA, Bathols, J (2007). *Bushfire Weather in Southeast Australia: Recent Trends and Projected Climate Change Impacts.* Bushfire CRC, Bureau of Meteorology & CSIRO.

Schuster S., Blong R. J., Leigh R. J., and McAneney K.J. (2005) 'Characteristics of the 14 April 1999 Sydney hailstorm based on ground observations, weather radar, insurance data and emergency calls'. *Natural Hazards and Earth System Sciences,* 5, 613–620

B RNT Ministerial Directions

C Memorandum of understanding

D RNT information technology assets

Table 18 Components of RNT IT infrastructure hardware

Component	Function
RNTServer	This is the Primary Domain Controller and runs Windows Small Business Server 2011. This server also runs the RNT's messaging infrastructure on Exchange Server 2010. The user mailboxes, Public Folder databases and transaction log files are all stored on the data volume of the server.
MapServer	This server is used for file sharing. It is connected to the Domain Controller as a member server.
Tape Drive	A tape drive (HP StorageWorks Ultrium 2860 SAS) is installed in the data cabinet and attached to the server. It backs up daily to data cartridges which are ejected automatically every morning.
External Hard Drive	The external hard disk is attached to one of the servers and stores updated copies of images of both servers every week.
Personal computers	There are 5 HP desktops model PC 2210 workstations in the offices. Three of the computers are used by the RNT permanent staff, while a fourth contains MYOB and is used by an accountant from CMCT. There is one spare desktop computer.
Phone system	There are 6 desktop phones model LG Nortel and Aria
Multifunction device	The model is a Canon C5051 and it is mapped on each user's PC as the default printer. It has a fax card as well as a scanner function.
Security system	This is a Digiport Security System and there are two cameras mounted at the Waroona and EastGate sides of the cemetery. The monitoring console is located in the main room of RNT.

Table 19 RNT Software

Device	Software components
Server	Windows Small Business Server 2011 MS Exchange 2010 Veritas Backup Exec Kaspersky Anti-Virus for Servers Kaspersky Anti-Spam email filtering

Device	Software components
Computers	Windows 7 operating system on all PCs Microsoft Office 2013 application for all document processing and email functions MYOB for accounting purposes Kaspersky Anti-Virus for security on all PCs. The anti-virus signatures are updated automatically over the internet. FileMaker database program for saving all maps and project data

E Key contacts

Table 20 Key RNT stakeholders

Organisation	Position	Contact	Phone / email
Department of Primary Industries	Minister	The Honourable Katrina Hodgkinson	02 8574 6200
CMCT	Chief Executive Officer	Peter O'Meara	02 8713 5700
RGCRT	Chief Executive Officer	Fiona Heslop	02 9746 2177
Invocare	Operations Manager	Kevin Morgan	02 9746 8945
War Graves Commission	Area Manager	Geoff Taplin	02 9746 5565

Table 21 External RNT management support

Role	Organisation	Contact	Phone
IT Support	A2K Technologies	Jason Mainwaring	0404 831 825
Accounting	Catholic Metropolitan Cemeteries Trust	Dave Renneberg (CMCT)	02 8713 5700
Financial advice/ management consulting	CMCT and RGCRT Chief Financial Officers	Dave Renneberg (CMCT) Kevin Smith (RGCRT)	02 8713 5700 02 9746 2177
Infrastructure support	Triaxial Consulting	Jeff Knox	0403 154 871

F Funeral notification template

The Rookwood Necropolis Trust has the responsibility of the overall management of Rookwood Cemetery. In order to support our oversight of the site, we would appreciate it if you could please use this template to notify the RNT if a significant or controversial funeral has been organised. That is a funeral likely to generate significant media attention/ cause a major disruption/ involve a police presence or otherwise be considered of public interest.

Organisation: -

Name: - - - - - - - - - - - - - - - - - - Contact no/ email : - - - - - - - - - - - - - - -

Funeral date: - - - - - - - - - - - - - - - - Deceased name: - - - - - - - - - - - - - - - -

How many people are likely to attend the funeral? - - - - - - - - - - - - - - - -

Are media going to be present? □ Is a police presence likely? □

Could you please note any special arrangements that have been made for the funeral:

- -

- -

- -

- -

- -

- -

G Insurance

The RNT insurance requires review and updating to ensure that adequate and comprehensive cover is provided for staff, assets and personal liability in the event of a major incident.

Table 22 RNT insurance 2014-2015

Insurance type	Insurer name	Policy number	Policy value	Policy renewal date
Motor vehicle	ALLIANZ	80ROO0341VSD	Market value	04/04/2015
Business Pack Ins – Incl Public Liability	QBE	1ANA887573BK	$50,000,000	26/08/2015
Statutory liability				
TMF insurance				
Volunteers				
Workers compensation	GIO	WC127143157		30/06/2014
Other Lot 493 House	GIO	HGL005090529	$863,000	26/04/2015