Caring for our People

As we’ve been preparing for our Resources Open Day, we’ve been imagining what visitors to the Synod office might be expecting. The nature of our ‘business’ side of the church and our focus on ‘dollars and cents’ means that people might associate us with forms to fill in, bills to be paid and compliance with legislation which seems over engineered for the small teams serving congregations.

We’ve found ourselves in conversation about the values that underpin what we do. As the church we are ‘called to care’ and this means caring for the vulnerable and the disadvantaged, often outside our congregations, but it also means caring for, valuing and respecting one another.

Our Human Resources and Work Health Safety staff see their strong compliance and regulation focus as being one of the ways the church articulates how it goes about caring for its people. We believe that how the church treats its own people should exceed, not just meet, minimum requirements. We exercise this call to care through seeing good practices are followed and striving to make sure all congregation members, volunteers or paid staff are cared for, valued and respected. We believe this is exercising good stewardship of people and the gifts they bring as we serve the church together.

Peter Battersby
Executive Officer, Resources

Synergy

Synergy coordinates solutions to some of the common purchasing and contracting requirements of Uniting Church organisations to obtain the best value on a range of products and services.

Jointly funded and managed by representatives from Uniting Church and UnitingCare organisations, Synergy aims to ensure the good stewardship of scarce resources and draws on the combined expertise within Uniting Church networks to ensure competitive prices and conditions are accessible to all parts of the Church including staff and volunteers.

Organisations that have participated in Synergy recognise the less tangible benefits arising as well as the financial benefits realised. Working collaboratively on Synergy projects provides the opportunities to share information, expertise and build relationships. Church congregations can benefit from information that organisations and schools have provided through Synergy.

Some of the contracts that Synergy manage include Air Conditioning Scheduled Maintenance, Managed Linen, Nursing Agency Staff, Fire Equipment Scheduled Maintenance, Energy and much more.

We also provide a variety of staff benefits, accessible to staff and volunteers of Uniting Churches, Schools and UnitingCare organisations in SA, including IT, whitegoods, car hire and groceries.

Visit our website www.synergy.unitingcare.org.au for more information or contact Kylie Dayman, Synergy Manager via synergy@sa.uca.org.au or (08) 8236 4263 if you wish to engage Synergy for your purchasing needs.
property services

“Synod owns our property” – or does it?

The words “the Synod owns our property anyway” are often said – but is this true? Actually, no – all property is vested in the Uniting Church in Australia Property Trust (S.A.) on behalf of the whole Church, that is, all the Uniting Church members in the South Australian Synod’s boundaries (most of S.A.).

Legal entity for property

The Property Trust is the legal entity for all property – including Congregational property, Synod property and Uniting Church bodies (e.g. Historical Society, Uniting College of Leadership & Theology etc.). The local congregation, Uniting Church body or the Synod is the custodial user of a particular property. It can be likened to being a life tenant – where the life tenant has the enjoyment and use of the property together with the responsibility to maintain and care for the property.

The “commonwealth” of property

The Property Trust is a body corporate, created by an Act of Parliament in 1997 at the inauguration of the Uniting Church. The Trust holds property as “commonwealth” on behalf of the whole church for worship, witness and service. Common, meaning “belonging to all”, and wealth, meaning “happiness or riches”, the word commonwealth has come to mean any government in which all people involved have a say. In Uniting Church governance, all members have the opportunity to have a say through the various councils of the Church including meetings of the Congregation, Elders’ Leaders’, Presbytery, Synod and Assembly.

Sale of property

All property is sold as per the Regulations and the process outlined in the Property By-law and the Property Sale Proceeds Policy. Properties are not an asset on a Congregation’s balance sheet and similarly, when properties are sold, any sale proceeds available to the Congregation as per the “category of sale” are held by the Property Trust on behalf of the Congregation for approved purposes.

Theology of property

Although the work of God in Jesus Christ through the Holy Spirit is not bound to property, the Church, through the Property Trust, has acquired properties over many years as places to gather as the people of God. Hence the Church has bound itself to property. But the Church is still the Church with or without property. The Church can be separated from property but the property of the Church can’t be theoretically thought of apart from the Christian community in worship, witness and service.

Purpose of property

“Form follows function”, (a misquote of “form ever follows function” by architect Louis Sullivan in the 1890s), speaks about the planning of a building being based on the function of the building, not the form of the building dictating what function will be into the future. As form follows function, property follows mission. Mission should be the driving factor for any and all property issues. Property is a means to an end and not an end in itself – the ‘trim’; the purpose and function, being the proclamation of the gospel. The church should not be driven by buildings but exists to serve God and participate in God’s mission in the world.

Responsibility for property

The Church Council is responsible for the management and administration of all church property acquired or held for the use of the Congregation (Regulation 4.4.1). Further information regarding the responsibility for property can be found in the Regulations at http://sa.uca.org.au/property-services/.

(Note: For commercial leases, residential leases, licence agreements and all property transactions, the legal entity is the Property Trust and documentation must be in the name of the Property Trust.)

Final words on property

So back to property ownership – Synod doesn’t own all our property, the Property Trust owns all Uniting Church property on behalf of all members of the Uniting Church.

- Agreement – this should be discussed, accepted and signed by both the Employment Provider and the Host organisation.
- Subcontractor – a Host cannot subcontract any part of the WfD program without the approval of the Employment Provider.
- Host – this will be the Church Council on behalf of the congregation and this cannot be a subcontractor. Hosts effectively become the lead contractor and accept the main WHS duties and responsibilities, particularly for supervising workers, training and any subcontractor providing professional services. Hosts are also required to ensure that any works undertaken meet the relevant building codes and/or heritage requirements. If your project includes property improvements which are valued over $10k, requires Development Approval, impacts heritage requirements or affects the structure of the property, you should discuss the proposed work with Property Services in the early stages of planning.
- Employment Provider – the government approved agency who arrange and administer the program. They will approve and sign the agreement, and require ongoing information relating to attendance etc. be forwarded to them.
- WfD Coordinator – appointed to secure and provide the link between the Employment Provider and the Host organisation.

If your congregation has found any damage as a result of the storms, please contact Insurance Services as soon as possible and we can advise you of any claims process.

Wayne Booth

WHs Safe-Tea Break

Welcome to the final instalment of Safe-Tea Break for 2016 - and my ongoing quest to try and demystify WHS. In this article I’m again focussing on the ‘Duties and Responsibilities’ theme and hopefully clarifying how this extends to different types of activity in the church and in particular ‘Work for the Dole’. In the previous edition I focussed on contractors in general and thought it might be useful to clarify a congregation’s duties when hosting a Work for the Dole (WfD) activity.

A number of our congregations have sought to, begin and even completed WfD projects; they can be a beneficial way of undertaking work in a church that might otherwise have few other options. Whether this is much needed decoration, grounds keeping, general building improvement works or even additional admin support, the potential benefits can appear very attractive.

However, before becoming a host for this programme, a Church Council must ensure the proper consideration and due diligence is given. The following is provided as a brief guide intended to help with this:

- Host - this will be the Church Council on behalf of the congregation and this cannot be a subcontractor. Hosts effectively become the lead contractor and accept the main WHS duties and responsibilities, particularly for supervising workers, training and any subcontractor providing professional services. Hosts are also required to ensure that any works undertaken meet the relevant building codes and/or heritage requirements.
- Host - this will be the Church Council on behalf of the congregation and this cannot be a subcontractor. Hosts effectively become the lead contractor and accept the main WHS duties and responsibilities, particularly for supervising workers, training and any subcontractor providing professional services. Hosts are also required to ensure that any works undertaken meet the relevant building codes and/or heritage requirements.
- Host - this will be the Church Council on behalf of the congregation and this cannot be a subcontractor. Hosts effectively become the lead contractor and accept the main WHS duties and responsibilities, particularly for supervising workers, training and any subcontractor providing professional services. Hosts are also required to ensure that any works undertaken meet the relevant building codes and/or heritage requirements. If your project includes property improvements which are valued over $10k, requires Development Approval, impacts heritage requirements or affects the structure of the property, you should discuss the proposed work with Property Services in the early stages of planning.
- Employment Provider – the government approved agency who arrange and administer the program. They will approve and sign the agreement, and require ongoing information relating to attendance etc. be forwarded to them.
- WfD Coordinator – appointed to secure and provide the link between the Employment Provider and the Host organisation.
- Subcontractor – a Host cannot subcontract any part of the WfD program without the approval of the Employment Provider.
- Host - this will be the Church Council on behalf of the congregation and this cannot be a subcontractor. Hosts effectively become the lead contractor and accept the main WHS duties and responsibilities, particularly for supervising workers, training and any subcontractor providing professional services. Hosts are also required to ensure that any works undertaken meet the relevant building codes and/or heritage requirements.
- Host - this will be the Church Council on behalf of the congregation and this cannot be a subcontractor. Hosts effectively become the lead contractor and accept the main WHS duties and responsibilities, particularly for supervising workers, training and any subcontractor providing professional services. Hosts are also required to ensure that any works undertaken meet the relevant building codes and/or heritage requirements. If your project includes property improvements which are valued over $10k, requires Development Approval, impacts heritage requirements or affects the structure of the property, you should discuss the proposed work with Property Services in the early stages of planning.
- Employment Provider – the government approved agency who arrange and administer the program. They will approve and sign the agreement, and require ongoing information relating to attendance etc. be forwarded to them.
- WfD Coordinator – appointed to secure and provide the link between the Employment Provider and the Host organisation.
- Subcontractor – a Host cannot subcontract any part of the WfD program without the approval of the Employment Provider.
- Host - this will be the Church Council on behalf of the congregation and this cannot be a subcontractor. Hosts effectively become the lead contractor and accept the main WHS duties and responsibilities, particularly for supervising workers, training and any subcontractor providing professional services. Hosts are also required to ensure that any works undertaken meet the relevant building codes and/or heritage requirements.
For important cut-off times relating to the Payroll Bureau (for December and January pay cycles) please see the Payroll section in this newsletter.

UCSA Screening Services Unit – using the correct Police Check application form
Please ensure that persons requiring a UCSA police check (new checks or renewals) use the current application form.

Applicants should read and follow the instructions included on the form and ensure that original ID documents are checked and correctly witnessed by an authorised person i.e. UCA Ministers, UCA employees or members of UCA Church. (Please note that authorised persons for the purpose of this check does not include JPs or Police Officers).
Details of where an applicant is volunteering/working and also the role and duties being undertaken must also be included where indicated. This information is required in order to process the application.

This is a fillable form into which you can type your details online before printing it off to sign and send in.
If you have any questions, please call 8236 4270 or email screening@sa.uca.org.au

Australian Charities and Not for Profit Commission (ACNC)
The Annual Information Statement (AIS), required by the ACNC, must be lodged with them no later than 6 months after the end of your financial year.

For congregations with a 30 June end of year, this should be lodged with the ACNC by 31 December.
Please see the link below for further assistance.

Uniting Church SA - ACNC

Payroll
December Payroll cut-off times
December is a significantly shortened working month so we ask that all timesheets and leave forms are submitted to the Payroll Bureau as soon as possible and no later than Thursday 1st December. This will greatly assist Payroll in completing the pay cycle and all other obligations on time.

Please note, any leave reflected on December timesheets or planned to be taken in December should be accompanied by an authorised leave form. Timesheets & leave forms can be scanned & emailed to payroll@sa.uca.org.au or posted or faxed.

If you have any questions, please don’t hesitate to contact Payroll by emailing payroll@sa.uca.org.au or phone 8236 4241 or 4242.

Ransomware: a type of malicious software designed to block access to a computer system and/or files until a sum of money is paid

With the Synd Office having had a recent experience with this type of software we thought it timely to send out some tips to help everyone protect their computers and information. In our case a convincing email claiming to be from a well-known company tricked one of our users into clicking a link to view a consignment note. Once the link was clicked this downloaded the ransomware which got to work straight away and encrypted all of the files that our unsuspecting user had access to (including network files). It then left a message with instructions on how to pay the ransom to get the file decrypted.

As we have a robust backup regimen, data loss was minimised to 2 hours and some lost work time whilst the files were being restored. Whilst this was unfortunate, we were very lucky that we could do this and did not have to pay the ransom. It’s worth noting that paying the ransom does not always guarantee that the files can be decrypted as this depends on the honesty of the ransomware creator - which may be questionable!

Our recommendations to protect yourself are:

1. Install a good virus scanner and keep this up to date (both the program and virus definitions)

Whilst this won’t stop all ransomware (as antivirus is always one step behind the creators of ransomware), it’s a good start and will also protect against other threats. There are plenty of good, free and paid virus scanners available, and some (like FortiClient) also protect against other threats. There are plenty of good, free and paid virus scanners available, and some (like FortiClient) also

2. Learn how to spot fake emails

Almost anyone can fake an email to look like it has come from a legitimate source and these are not dangerous in themselves, it’s the links or attachments within them that are the problem.

- Never open attachments from unknown sources. If in doubt call the sender to verify the email, if they know nothing about the email delete it immediately.
- Be careful clicking on a link from within an email. Most email programs will display the web address when you hover the mouse pointer over the link (without clicking). If the web address looks suspicious delete the email immediately.

More information can be found here: https://blog.mimipath.com/10-tips-on-how-to-identify-a-phishing-or-spooing-email-

3. Make regular backups of your files and store these off-line

Microsoft have a built in backup program in their operating systems or simply copying your files to an external hard drive every other day will suffice. The amount of data, how often it is changed, and what you can live without will determine how often you should be backing up. USB sticks can sometimes be unreliable so they are not recommended as a backup media.

Keeping the files off-line means not having them accessible from your computer. An example would be storing an external backup drive in a filing cabinet. If your computer is affected by ransomware, the files on your off-line drive are still safe. If the external drive spends all its time plugged into your computer (i.e. online) you risk your backups being encrypted along with the rest of your files leaving you with no choice but to either pay the ransom or live without your files.

Payroll Bureau Administration Processing Fee increase - 2017
The Payroll Bureau Service Fees will be increasing from 1st January 2017 in order to partially recover costs associated with providing the Payroll Bureau Service. The new rates are listed below:

Excluding GST Including GST
Payroll Monthly Admin Fee $20.10 $22.10
Set up of New Company $104.55 $115.00
Set up of New Employee $52.27 $57.50
Termination of MOU Fee $26.13 $28.75
Reprocessing Fee $26.13 $28.75
Recovery Fee (Payment Summary) $46.90 $51.59

Information Technology and Telephony

Ransomware: a type of malicious software designed to block access to a computer system and/or files until a sum of money is paid

With the Synd Office having had a recent experience with this type of software we thought it timely to send out some tips to help everyone protect their computers and information. In our case a convincing email claiming to be from a well-known company tricked one of our users into clicking a link to view a consignment note. Once the link was clicked this downloaded the ransomware which got to work straight away and encrypted all of the files that our unsuspecting user had access to (including network files). It then left a message with instructions on how to pay the ransom to get the file decrypted.

As we have a robust backup regimen, data loss was minimised to 2 hours and some lost work time whilst the files were being restored. Whilst this was unfortunate, we were very lucky that we could do this and did not have to pay the ransom. It’s worth noting that paying the ransom does not always guarantee that the files can be decrypted as this depends on the honesty of the ransomware creator - which may be questionable!

Our recommendations to protect yourself are:

1. Install a good virus scanner and keep this up to date (both the program and virus definitions)

Whilst this won’t stop all ransomware (as antivirus is always one step behind the creators of ransomware), it’s a good start and will also protect against other threats. There are plenty of good, free and paid virus scanners available, and some (like FortiClient) also have the added bonus of being able to block malicious websites.

2. Learn how to spot fake emails

Almost anyone can fake an email to look like it has come from a legitimate source and these are not dangerous in themselves, it’s the links or attachments within them that are the problem.

- Never open attachments from unknown sources. If in doubt call the sender to verify the email, if they know nothing about the email delete it immediately.
- Be careful clicking on a link from within an email. Most email programs will display the web address when you hover the mouse pointer over the link (without clicking). If the web address looks suspicious delete the email immediately.

More information can be found here: https://blog.mimipath.com/10-tips-on-how-to-identify-a-phishing-or-spooing-email-

3. Make regular backups of your files and store these off-line

Microsoft have a built in backup program in their operating systems or simply copying your files to an external hard drive every other day will suffice. The amount of data, how often it is changed, and what you can live without will determine how often you should be backing up. USB sticks can sometimes be unreliable so they are not recommended as a backup media.

Keeping the files off-line means not having them accessible from your computer. An example would be storing an external backup drive in a filing cabinet. If your computer is affected by ransomware, the files on your off-line drive are still safe. If the external drive spends all its time plugged into your computer (i.e. online) you risk your backups being encrypted along with the rest of your files leaving you with no choice but to either pay the ransom or live without your files.