YWAM Scotland Data Protection Policy

Context and Overview

Key Details

- Policy prepared by: Becky Kremer
- Approved by board/SLT on: 11 June 2015
- Policy became operational on: 19 June 2015
- Next Review Date: 1 June 2017

Introduction

Youth With A Mission Scotland Ltd (YWAM Scotland) needs to gather and use certain information about individuals.

This can include donors, applicants, teachers, suppliers, church contacts, trainees, staff volunteers, volunteers, referees and other people we have a relationship with or may need to contact.

This policy and the related procedures describe how this personal data must be collected, handled and stored to meet the charity's data protection standards – and to comply with the law.

Why this policy exists

This data protection policy ensures that YWAM Scotland:

- Complies with data protection law and follows good practice guidelines
- Protects the rights of all our volunteers, donors and contacts
- Is transparent about how it stores and processes individuals' data and uses standard, approved statements about data protection wherever data is collected
- Honours the privacy of our data subjects by using their data for the purpose it was collected unless permission is given otherwise and not selling or transferring data to third parties
- Protects itself from the risks of data breach
- Only holds data for prescribed charitable purposes - these are personnel and trainee administration; donor and accounting recordkeeping; advertising, marketing and public relations; fundraising and charity objectives
- Has established standards for all staff, volunteers, and trustees to safely collect, use, store and destroy data they need for work that they are expected to uphold
- Prioritises data protection and provides a rhythm for managing our data, updating our policies and revising our practices

Data Protection Law

The Data Protection Act 1998 describes how organisations – including YWAM Scotland – must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be kept any longer than necessary
6. Processed in accordance with the rights of the data subjects
7. Be protected in appropriate ways
8. Not be transferred to countries outside the EU without adequate protection

Definitions, risks and responsibilities

Policy scope

This policy applies to:

- YWAM Scotland's national leaders and trustees
- All bases and teams of YWAM Scotland
- All staff, volunteers and trainees of YWAM Scotland
- All other people working on behalf of YWAM Scotland

It applies to all data that the charity holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. It covers both facts and opinions about the individual. Broadly, this is anything that would identify a living individual like contact details but also comments made about them in writing (on paper or electronically) such as evaluations or pastoral discussions. Data can include:

- name, address, email address and telephone
- nationality and passport details
- visa details, if applicable
- national insurance number
- start date and position within Youth with a Mission
- next of kin and contact details
- medical information
- physical or mental health records including disabilities or infirmities
- church affiliation and Christian experience
- career history/previous employment and professional expertise

- previous experience with Youth with a Mission
- references
- Protection of Vulnerable Groups (PVG) certificate , if applicable
- Self-disclosures of offenses
- racial or ethnic origins of the data subject
- political opinions, religious beliefs or other beliefs of a similar nature
- trade union, committee or professional body membership
- sexual life including sexual orientation
- any proceedings for any offense committed or alleged to have been committed
- Physical description, habits, personality, or character
- Public offices held
- Publications
- Student records, student financial records
- Application assessments, staff appraisals and disciplinary proceedings

As some of data held will be sensitive personal data, there are special considerations for its processing and storage. This policy also covers this and details are laid out in the Appendices and Procedures.

Data Protection Risks

This policy helps protect YWAM Scotland from some very real data security risks, including:

- **Breaches of confidentiality**. For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should understand and be free to choose how the charity uses data relating to them.
- **Reputational damage.** YWAM Scotland could suffer if hackers gained access to sensitive data or were seen to misrepresent why we collect or how we use it.
- **Loss of data.** For instance, IT equipment is not disposed of safely or data users do not transfer and delete data before leaving YWAM Scotland.

Responsibilities

Everyone who serves with YWAM Scotland has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy, and the relevant procedures, and data protection principles. However, the following people have key areas of responsibility:

- The **board of directors** is ultimately responsible for ensuring that YWAM Scotland meets its legal obligations.
- The **Data Protection Officer**, currently Becky Kremer, is responsible for:
    - Keeping the board updated about data protection responsibilities, risks and issues.

- Reviewing all data protection procedures and related policies, in line with an agreed schedule and submitting changes to the SLT for approval.
- Providing data protection training and advice for the people covered by this policy.
- Handling data protection questions from anyone covered by this policy.
- Dealing with requests from individuals to see the data YWAM Scotland holds about them (also called a subject access requests).
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- Evaluating and making recommendations for any third-party services the charity is using to store or process data such as cloud computing services.
- Approving data protection statements for all means of collecting data.
- Investigating data breaches.

- The **Team/Base Leaders** are responsible for:

  - Naming a Data Protection Champion/IT Manager to fulfil these responsibilities, if possible.
  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards. This includes cloud-computing services.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.
  - Implementing a virus protection plan.
  - Safely disposing all IT assets holding personal data.

- The **School Leaders/Recruiters/Communications Team** are responsible for:

  - Ensuring all forms used to collect personal data including applications, web forms, mailing list sign-ups, etc, include an updated and appropriate data protection statement.
  - Overseeing any recruiting, marketing and fundraising functions to ensure only authorised personnel access personal data and that data is destroyed promptly when no longer required.
  - Ongoing training with school staff to raise awareness of data protection issues related to trainees and to create a culture of respect and confidentiality.

- Any staff members with **Finance or Fundraising functions** are responsible to:

  - Alert donors or potential donors how their data will be used and provide an opportunity to opt-out of being stored in a donor database using current data statements (see Procedures).
  - Honour donors' requests for handling their data.
  - Keep accurate and up-to-date records.

- The **National Leadership Teams** (NLT and SLT) are responsible to:

  - Provide or ensure the provision of data protection training for all staff members and/or others acting on YWAM Scotland's behalf.
  - Designate officers to oversee data protection for the charity.
  - Report data breaches to the board, and the ICO if required.

- **Every staff member** is responsible to:
    - Read and understand the data protection policy. Ignorance is no protection if you find yourself in breach of the Act.
    - Review your own personal data protection plan – especially if you hold sensitive or personal information on a portable device.
    - Follow the guidance and requirements of this policy to ensure the personal data you use for work is stored, used and destroyed safely.
    -

General staff guidelines

The only people able to access data covered by this policy should be those who need it for their work.

Follow the need-to-know rule. Only ask for, look at, store and share data you – or they – need for work.

Data **should not be shared informally**. When access to confidential information is required, staff members can request it from the department leader who holds it.

YWAM Scotland will provide training to all staff members to help them understand their responsibilities when handling data. Staff members are responsible to attend training.

Staff should keep all data secure by taking sensible precautions and following the guidelines in this policy and relevant procedures.

If a staff member holds YWAM data on their personal device, mobile devise usage guidelines must be followed including password access and file encryption.

To safeguard YWAM data, **strong passwords must be used** and they should never be shared.

Personal data **should not be disclosed** to unauthorised people, either within YWAM Scotland or externally. If in doubt, get permission from the data subject to share it.

Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be safely destroyed.

Staff members should **request help** from their line leader or the data protection officer if they are unsure of any aspect of data protection.

When a member of staff leaves YWAM Scotland or changes roles, promptly transfer or destroy data, change passwords and close redundant access codes and accounts.

YWAM Scotland Data Protection Procedures

Key Details

- Procedures prepared by: Becky Kremer
- Approved by board/SLT on: 11 June 2015
- Procedures became operational on: 19 June 2015
- Next Review Date: 1 December 2015

Procedures Included

- Data storage
- Data use
- Data accuracy
- Data destruction
- Subject access requests
- Disclosure for other reasons
- Data breaches

Appendices

- Data Protection Statements – approved for use
- Application Handling
- Handling Donations and Payments
- Fundraising and Marketing
- Building Your Data Protection Plan
- Remote Application Handling

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the data controller or data protection officer.

Paper storage & hard copies

When data is stored on paper, is should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in an inconspicuous, locked drawer or non-portable filing cabinet or secured storage room** (with designated, authorised key holders.)
- Staff should make sure paper and printouts are **not left where unauthorised people could see them**, like on a copier or printer.
- **Data printouts should be shredded or burned** and disposed of securely when no longer required.

Electronic Storage

When data is stored electronically, we must take reasonable measures to protect it from unauthorised access, theft, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between staff members. This also applies to any personal mobile devices that may contain YWAM data.
- If data is stored on **removable media** like a CD, DVD or USB drive, these should be kept **locked away securely** when not being used.
- Data should only be stored on designated computers and servers and should only be uploaded to a YWAM Scotland-approved cloud computing service.
- When local servers are used, the **servers should be in a secure location** away from general office space.
- Data should be **backed up frequently**. Backups should also be stored and deleted properly.
- Data **should not be saved directly to personal mobile devices** except in limited circumstances. Refer to the YWAM mobile device policy for further guidelines. Where remote access is required, an approved cloud-based service is the better option.
- All servers and computers containing data should be protected by **approved security software**.

Data use

Personal data is of no value to YWAM Scotland unless the charity can make use of it. However, it is when personal data is accessed and used that it be at the greatest risk of loss, corruption or theft.

- When working with personal data, staff members should ensure the **screens of their computers are always locked** when left unattended.
- Adopt a **clean-desk policy** so that personal data is never left open and unattended on your workspace.

- Personal data **should not be shared informally.** Unsecured, unencrypted emails and public phone conversations are two high-risk ways of sharing data that could easily result in unauthorised access to data. Use a cloud service, encrypt emails and/or speak privately on the phone as required.

- Discussing information known from personal data held by us might also lead to inappropriate disclosure. **Limit discussions of data with a "need-to-know" rule**. For instance, DTS staff processing applications need to discuss applicants' data freely with each other as they select trainees for a school. Base staff need to know special needs of volunteers to plan meals and housing assignments. Should pastoral or other needs arise outside the normal use and duties, **ask permission of the data subject to share the information further**.

- Personal data should **never be transferred outside of the European Economic Area** for processing without the written consent of the data subject. For instance, we require written permission from a trainee or staff member to pass on any information we hold about them to YWAM locations in the USA. If you cannot get written permission, a note with time and date of the verbal permission should be kept.

- Staff members **should not create extra or unnecessary copies** of personal data. For example, limit the number of copies printed of application forms.

- Do **not save copies of YWAM personal data to your own computer**. This includes application forms to be reviewed, mailing lists, databases, appraisals, discussions about applicants/staff, etc. Where this is necessary for remote workers, refer to the policy on the use of mobile devices.

- Always access and **update the central copy** of any data.

Specific data use policies have been created for some of YWAM Scotland's regular data processing functions. If you do any of the following, please read and apply the guidelines found in the appendix for:

- Processing applications
- Pastoral issues arising
- Fundraising and marketing
- Handling donations
- Mobile device usage

Data accuracy

The law requires YWAM Scotland to take reasonable steps to ensure data is kept accurate and up to date and it is the responsibility of all personnel to do so.

The more important it is that the personal data is accurate, the greater effort YWAM Scotland should put into ensuring its accuracy.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets. This limits the opportunity for un-updated data to be in use.
- Staff should **take every opportunity to ensure data is updated**. For instance, by confirming a donor's details when they call.
- Where possible, YWAM Scotland will **make it easy for data subjects to update** the information held about them. For instance, through a web portal.
- Data should be **updated as inaccuracies are discovered**. For instance, if mail is returned "address unknown" or stored telephone numbers are inactive, the data should be removed from the database.

Data destruction

Destruction Schedule

Data must only be kept as long as required and safely destroyed. Please refer to the following schedule for data destruction:

Financial Records:	Destroy after 7 financial years
Basic Personnel Record*:	Destroy after 40 years
Trainee Records & Applications:	Destroy 6 months after leaving YWAM Scotland
Staff Records & Applications:	Destroy 6 months after leaving YWAM Scotland
Incomplete or Denied Applications:	Destroy 6 months after no longer active
Background/PVG Certificates:	Log relevant details and destroy immediately
Regular Data Checkups:	MARCH & SEPTEMBER – destroy any expired data

*see Appendix 2

Safe Destruction

These guidelines refer to devices owned by YWAM Scotland and personal devices in use that also hold YWAM data.

Photocopiers and scanners with memory cards

- Remove memory cards and physically destroy or obtain a Data Destruction Certificate from the removal company. Store certificate with the team administrator.
- Paper files
- Authorised personnel who hold data may burn and oversee complete destruction of paper files or destroy in a cross cut shredder and safely dispose.

Electronic files – device no longer in use

- Hard drive must be deleted and wiped or completely physically destroyed. This is the responsibility of the individual owning/using the computer. Keep a log of the destruction of YWAM Scotland property with the team administrator.
- All IT assets that are being recycled, sold or returned to a leasing company must be cleared of personal data. So we don't find ourselves in breach of the Act, see the ICO's guidance here: https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf

Electronic files – device still in use

- Find all the locations on your device where the data files to be destroyed are stored. Delete the data. Ensure the data cannot be reconstructed by wiping the new free space. Refer to your operating system's instructions for secure deletion. The Information Commissioner's Office provides advice on deleting personal data: https://ico.org.uk/media/fororganisations/documents/1475/deleting_personal_data.pdf

Subject access requests

- All individuals who are the subject of personal data held by YWAM Scotland are entitled to:
- Ask **what information** the charity holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the charity is meeting its data protection obligations.

If an individual contacts the charity requesting this information, this is called a subject access request.

Subject access requests from individuals should be made in writing to the registered office address or by email to info@ywamscotland.org addressed to the data controller.

The data controller will aim to provide the relevant data within 14 days and will advise if there are any costs to provide the information. (Not more than £10 per subject access request.)

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Staff Requests

Under the 1998 Act, staff may also have access to their personnel files after giving 14 days notice in writing to the Personnel Department/Team Leader. Individuals may not take anything out of their Personnel file.

Confidential references are exempt from this aspect of Data Protection Legislation. However, on our references we do ask whether we may share them with the individual concerned. If express permission, in writing or email, has been obtained, these may also be shared. (If permission is given verbally, a record of that needs to be made in the individual's file including time and date of conversation – written consent is always better.)

Disclosing data for other reasons

In certain circumstances, the DPA allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, YWAM Scotland will disclose the requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Data breaches

An individual may complain to the Information Commissioner or directly to us about the way we handle data. We may also become aware of a data breach through inappropriate disclosure, loss or theft of data, loss or theft of a portable device holding data or inappropriate use of data.

- It is our duty to report a data breach to the data protection officer who will then begin an investigation.

The ICO expects organisations to investigate breaches and complaints. The extent and circumstances of the breach as well as the potential impact should be carefully looked at and considered.

- If the breach is serious or large, it may require us to report it to the ICO who may then launch their own investigation.

Adherence to the Data Protection Act is a condition of ongoing association with the charity. Any breaches of the Act will be taken very seriously with potential consequences, i.e., disciplinary measures or dismissal.

If an individual suffers (primarily financial) damage because YWAM Scotland or someone working on our behalf breached the Act, they are entitled to claim compensation. This right can only be enforced through the courts. We may defend the claim for compensation on the basis that we took all reasonable care in the circumstances to avoid the breach. *(If it was shown that YWAM Scotland had not made sure that the individual controller was aware, or following, this Data Protection Policy there could be dual responsibility).*

Compensation can also be claimed where distress has been suffered in addition to damage or if the distress arises out of a contravention with respect to the processing of personal data for the purpose of journalism, artistic or literary purposes.

Breach investigation process

When a complaint arises from a data subject or a data breach is reported:

- If breach ongoing, emergency measures must be taken to stop data loss
- Other damage limitation steps may need to be taken by data protection officer
- The data protection officer will form a working group
- As necessary, other data subjects may need to be told of breach
- The data protection officer and the NLT will inform the board of breach
- The group will identify people to be interviewed and outline a process
- Interviews and circumstances of breach documented
- Workflow and storage conditions at site of breach examined
- Legal consultations will be made if necessary
- The group will assess if the ICO needs to be notified
- The group will file a full report containing evidence
- The group will give an extended report to the NLT with recommend disciplinary action and improvements needed to data protection policy & practice
- The NLT will decide and implement any disciplinary action
- The group will file an executive summary with the board
- The group will provide appropriate response to interested parties

APPENDIX 1 – Data Protection Statements

YWAM Scotland aims that all individuals are aware their data is being processed and that they understand:

- How their data is being used and how long we'll keep it
- How to exercise their rights

To these ends, it is our policy, as outlined above, that all forms or methods used to collect data contain a relevant data protection statement so individuals understand how we will use their data before they provide it. Choose the relevant statement from the list of approved statements below for your form.

APPLICATION FORMS

Purpose: Your application form will be used for the recruitment, selection and registration process for our training courses and/or volunteer staff positions. As you enrol or take up a staff position, we may use some of your data for personnel or course administration. If we need to, we will also use it to communicate with you and your referees during the process.

Privacy: Access to this form is restricted to YWAM Scotland staff responsible for the recruitment, selection and administrative process for the team or course that you are applying to join. We operate a need-to-know-only policy for your personal information that limits what information is shared with, for example, senior staff, UofN course registrars, immigration, travel agents and local regulators to help you successfully complete your training course or placement. We never sell your data to third parties and will not share it for other purposes without your consent.

Data Protection: This information will be securely retained by YWAM Scotland in accordance with Data Protection legislation. Unless the law or insurance providers require us to keep it longer, your information will be kept no longer than necessary for the stated purposes and no longer than 6 months after you cease your involvement with YWAM Scotland.

You may write to our registered office at any time to update your information, remove yourself from any mailing lists, or ask what data we hold about you and how we use it. YWAM Scotland is not responsible for the personal data held by third-party services such as Paypal that you might use as part of the application process.

Please initial here if you agree to YWAM Scotland using your personal data in this way:

Please initial here to stay updated by email on YWAM Scotland's projects and activities:

GENERAL CONTACT FORMS

In accordance with the Data Protection Act (1998) we hold the data you give to us securely and use it for the purpose you shared it with us such as recruitment, communications, accounting and donor relations. Data is held only as long as necessary for the purpose unless required for recordkeeping by law or our insurance providers. We never sell personal data and do not share with third parties without your consent. You can always write to us to find out more.

WEBSITE FORMS

When you submit a form on this site, all answers are held securely in accordance with the Data Protection Act (1998) and we do not collect data about you unless you give it to us. (Click to read our Cookie Policy.) We use your data for the purpose you shared it with us such as recruitment, communications, accounting and donor relations. Data is held only as long as necessary for the purpose unless required for recordkeeping by law or our insurance providers. YWAM Scotland never sells your personal data and does not share it with third parties without your consent.

Youth With A Mission Scotland Ltd is not responsible for the personal data held by third party services you may use to donate such as Paypal or give.net. You can always write to us to find out more.

(Click here to read our privacy policy.)

Cookie Policy:

This site uses cookies - small text files that are placed on your machine to help the site provide a better user experience. In general, cookies are used to retain user preferences, store information for things like shopping carts, and provide anonymised tracking data to third party applications like Google Analytics. As a rule, cookies will make your browsing experience better. However, you may prefer to disable cookies on this site and on others. The most effective way to do this is to disable cookies in your browser. We suggest consulting the Help section of your browser or taking a look at the About Cookies website which offers guidance for all modern browsers.

Giving:

If you make a financial gift to YWAM Scotland, we are required by law to collect and store some data for tax relief and audit purposes (usually up to 7 years). We hold and use the data in accordance with the Data Protection Act (1998). We also like to stay in touch with our donors to keep them updated on our work and future needs. Where possible, we will provide an opportunity for you to opt-out of your data being used for YWAM Scotland communications at the point of giving. You may write us at anytime to update the data we hold on you or to remove yourself from any mailing lists.

Youth With A Mission Scotland Ltd is not responsible for the personal data held by third party services you may use to donate such as Paypal or give.net.

PRIVACY POLICY

We do not collect your data unless you choose to give it to us. In accordance with the Data Protection Act (1998), we hold the data about you securely and use it for the purpose you shared it with us such as recruitment, communications, accounting and donor relations. We hold the data only as long as necessary for the purpose unless required for recordkeeping by law or our insurance providers.

If you have given us your contact details, we would like to respond to your enquiries and send you information about YWAM Scotland regarding our work, prayer or financial needs.

If you make a gift to YWAM Scotland, we are required by law to collect and store some data for tax relief and audit purposes. We also like to stay in touch with our donors to keep them updated on our work and future needs. Where possible, we will provide an opportunity for you to opt-out of your data being used for YWAM Scotland communications at the point of giving.

You may write us at anytime to update the data we hold on you, remove yourself from any mailing lists, or ask what data we hold about you and how we use it. YWAM Scotland never sells your personal information and we do not share with third parties without your consent.

Youth With A Mission Scotland Limited is not responsible for the personal data held by third party services you may use to donate or make payments such as Paypal or give.net.

If you have any other questions about our privacy policy, please be in touch.

APPENDIX 2 - Handling Applications

- Ensure you are using the latest version of the application form with an approved data protection statement on it.
- Designate an application processing team. These are your authorised personnel to handle applications. This might include a registrar who collates the applications, a medical officer, and two or three staff members to review and accept the applicants.
- When receiving and storing applications electronically, use a YWAM computer unless absolutely necessary. Access to the files must be password protected.
- When handling paper applications, avoid making duplicate files. When duplicates are necessary, destroy the duplicates immediately after no longer needed.
- When sharing computer access to read or process applications, separate - not shared - passwords should be used. This could be done by using a cloud service accessible to different authorised users on a computer or fully cloud-based with a YWAM-approved cloud service.
- (Within limits, having more than one person able to access the data can actually be helpful - it prevents loss of data in the event of death, incapacity or departure.)
- If data is stored directly on a computer's hard drive, disable removable media ports on data storage computers.
- Avoid sending applications by email unless using a YWAM-approved email encryption software. See Appendix 6 for tips on remote application processing.
- Backup the data regularly - once a week minimum. Follow safe storage procedures for back-ups as well.
- Put medical information in a sealed envelope marked CONFIDENTIAL in the paper file. Electronically it should be kept separately for the use of the designated medical person only.
- Capture the needed data from any background checks or PVG forms and keep a log of that information only. Destroy or return the background check/PVG certificate.
- When you are not actively using paper files, they must be kept in a locked filing cabinet/cupboard or room that is not shared as general office space. Key access should be limited and a key holder log kept with the team administrator.
- When a request is made for information from the application, remember the need-to-know rule. Only pass on the information your fellow workers need for their work.

- The summary form used for processing the application may be retained to form a basic personnel record. It should include the start date and the date involvement ends.

APPENDIX 3 - Handling donations and payments

- Follow the data protection policies and procedures – including electronic ones – when working with financial data.
- Ensure you are using the latest version of any giving forms with an approved data protection statement on it – as well as the latest Gift Aid information.
- Don't take information for a database or filing system that the donor/payee hasn't given us. (For example, copying addresses from a cheque or using another form they filled out to put in a donor database.)
- Give donors/potential donors an option to opt-out of staying on a mailing list or in a database if that's what you intend to do with their information.
- If someone opts-out, then honour their request.
- Don't record giving details to add someone to the database or mailing list if they are under 18.
- When someone contacts us to discuss their donation or personal information, confirm their identity. For example, if you have their address on file, ask them to tell you their address and match it to the file. Don't just tell them information and then ask if that's right.
- Take every opportunity to keep donors' information up to date. This might mean yearly mailings, confirming it when they contact us, web forms, etc.
- Keep a clean-desk or workspace. If you step away from your desk, keep sensitive financial information hidden or put away.
- Treat discussions about a donor's or payee's financial information, giving amounts, debts, etc, as confidentially as you would a pastoral issue. This includes discussions about payments from trainees, staff members, and applicants. Remember the need-to-know rule and keep discussions private. Take care on phone calls that may be overheard – get creative with code words or talk later.
- Never take the YWAM Scotland donor information for personal use or sell or share it with another party.
- Designate an application processing team. These are your authorised personnel to handle applications. This might include a registrar who collates the applications, a medical officer, and three staff members to review and accept the applicants.
- Keep to the destruction schedule.
- Do not store bank or credit card details unless the donor or payee authorises in writing for a specific purpose.

APPENDIX 4 - Fundraising and Marketing

Contact Acquisition

- If you want to gather information for a specific purpose tell people what you want, how you will use it, and how long you will keep it. Then – do just that.
- When using a sign-up sheet or form to gather info, include the appropriate and up-to-date data protection statement.
- When merging contact lists, be sure that the information was originally given in a way that matches how you want to use it now.
- Make a habit of putting the data subject in charge of how their data is used. For example, John works with New Church. He wants to be in touch with Sally who is on staff with us about an upcoming event. Instead of passing on Sally's data, ask John for his and give Sally the option to be in touch. This also works in reverse as we collect contacts!

Mailing Lists

- If it's been a while since you contacted people on a mailing list, highlight how they can opt out.
- Always provide an unsubscribe option.
- Never use a YWAM Scotland mailing list for personal use or sell or share it with another party.
- Use a mailing list for the purpose you collected it. That's it. If you want some flexibility for what you contact people about, be sure people know that from the beginning. You can do that by having a more general data protection statement wherever you collect contact details.

APPENDIX 5 Building your Data Protection Plan

Existing data

Are you currently holding any personal data?

- For what purpose are you holding it?
- Is it sensitive data?
- Does the individual know you are holding their personal data/have they given consent?
- Are there areas you could limit what you know or data you are accessing? In other words, do you REALLY need-to-know?
- Are you safely destroying redundant data in a timely manner?
- Do you have a data transfer plan in place if you leave your role or YWAM Scotland?

Do you comply with all aspects of this policy?

- Are all your electronic devices password protected and encrypted?
- Do you have data stored directly on your device that could be stored elsewhere or deleted?
- Are you regularly backing up your devices?
- Are any paper held records holding personal data stored in a locked cabinet and a locked room/building when unoccupied?
- When you work with data, are you protecting it from accidental disclosure, theft or loss?

Collection of new data

- Are you using the latest version of forms including the latest approved data protection statement?
- Other organisations also have data protection policies we must respect - don't take personal data from another organisation without the consent of the individual concerned.
- Are you making a habit of putting the data subject in charge of how their data is used?

APPENDIX 6 – Remote Application Processing

Sometimes, the application processing team is located across multiple locations. When this is the case, we need an alternative storage and handling protocol. In general, you should follow all safe application processing guidelines but the mechanics might change in how you do that.

- The lead person on the processing team should act as registrar. This may be the person receiving the applications or recruiting the personnel.
- The acting registrar should upload the files into their own separate and named folder on a cloud-based service such as Dropbox (YWAM Scotland approved.) Then this folder should be shared with only the other members of the processing team.
- Only relevant information should be uploaded – other reviewers do not need passport information, for example.
- If you received the application forms via email as an attachment, send a reply email confirming you received the forms and copy yourself – that way you can keep a copy of your email correspondence whilst deleting the email with the attachments once they become redundant.
- An evaluation form should also be uploaded in the folder.
- As the team reads and processes the application, it should only be opened from Dropbox and not downloaded or stored to any personal device.
- Comments on the application should be made on the evaluation form and saved within the Dropbox folder.
- Once the application has been fully processed and a decision made, the evaluation form can be printed by the registrar and added to the paper folder.
- The registrar should then remove all sharing on the folder and destroy/store the application safely. Where electronic storage is on a personal device, a data plan should be in place for destruction and/or continuity after the device is no longer in use or the holder changes roles.