DATA PROTECTION & CONFIDENTIALITY POLICY

(Including the General Data Protection Regulations)

CONTENTS

1. Introduction

1.1. The principle of this policy is to establish how Darlington Area Churches Youth Ministry (DACYM) conducts its business to ensure that it maintains the highest standards of confidentiality, and is compliant with law inregard to Data Protection.

1.2. Discussion on issues of confidentiality and data security will be encouraged both in team meetings and in supervision. The purpose of this is to increase the staff team's understanding of confidentiality and to ensure that confidentiality and protection of data is given a priority within the organisation.

1.3. Breaches in confidentiality or data security will be subject to disciplinary proceedings or, in the case of participants, some form of appropriate sanction or withdrawal of services.

1.4. Darlington Area Churches Youth Ministry (DACYM) respects the right to privacy of its present and former participants, staff, volunteers and supporters and will take all reasonable steps to protect personal informationgiven to us by all individuals.

1.5. This policy links directly to our Child Protection and Safeguarding Policy and our Adults at Risk Policy and attention must be given to the provisions of their contents when dealing with confidentiality and data protection.

1.6. In the UK, the Information Commissioners Office (ICO) is the independent body set up to uphold information rights.

2. Definitions

- **Personal Data:** information relating to a living individual, including expressions of opinion about that person
- **Processing:** this is widely defined to include almost anything you might do with data, including simply holding it on file.
- **Data subject:** an individual who is the subject of personal data.

3. Principles of the General Data Protection Regulations

3.1. The GDPR form part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018).

3.2. The GDPR set out seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

3.3. These principles therefore lie at the heart of our approach to processing personal data.

3.4. Any person who processes data must comply with the provisions of the Regulations. Processing includes obtaining, recording, manipulating, holding, disclosing and destroying data - so just about anything one can do with data amounts to processing.

3.5. In addition to the GDPR, the Privacy and Electronic Communications Regulations (PECR) relate to any marketing carried out by phone, fax, email or text.

3.6. The ICO has also made available specific guidance related to the processing of records relating to children and young people.

4. Data Controller

The nominated Data Controller is: Martin Stand (Project Director)

5. Board Member with responsibility for Data Protection (SIRO)

5.1. The Board will appoint from among its membership a person who is responsible for championing Data Protection, known as the Senior Risk Information Officer (SIRO).

5.2. The nominated SIRO is: Emily Carling

5.3. The SIRO will be responsible for:

- Annual reviews of the Data Protection policy and its implementation across the organisation.
- Working with the Data Controller to implement change or improvements where necessary.
- Investigating any alleged Data Breaches and reporting internally and externally as necessary.

6. Types of data that we process and the legal basis applied

6.1. Darlington Area Churches Youth Ministry (DACYM) is a data processor in respect of the records it keeps on clients (current,future and former), staff, job applicants (whether successful or unsuccessful), current and former employees, and supporters/donors.

6.2. There are 6 legal conditions on which we can hold and process data:

- Consent
- Necessary for Contract
- Legal obligation
- Vital interests
- Lawful authority (in the public interest)
- Legitimate Interest

6.2.a. Darlington Area Churches Youth Ministry (DACYM) only holds information on **supporters** with their consent. This consent must be explicit, opt-in consent, and we should be able to evidence when this was obtained and with what explanation (privacy notice).

6.2.b. Information held about **children, young people and other participants** is generally held in return for a service and is therefore under the Legitimate Interest condition.

6.2.c. **Donors** are often "supporters" as well and so information will be held with consent. However, if consent for marketing is not given, data may still be held regarding donations under the legal obligations of tax and charity law.

6.2.d. Information about **employees** will be kept as Necessary for Contract.

6.2.e. Records about **volunteers** will be kept as Necessary for Contract.

6.2.f. Records of **Trustees** are part of the public record of the charity and so will be kept indefinitely.

6.2.g. Records of unsuccessful **job applicants** will be kept for 1 year from the time of application and then destroyed.

6.3. In all cases, keeping records about people for specific purposes such as the above does not give automatic permission to process the data for the purposes of fundraising or marketing.

7. Individuals' access to their own Personal Data

7.1. Individuals have the right to:

- be informed if an organisation holds their personal data

- make a request to see what data the organisation holds about them and have access to such information within one month (there is a legal duty to respond to such requests)
- where appropriate, to have it corrected or erased

7.2. Darlington Area Churches Youth Ministry (DACYM) has different processes and data-deletion policies for different groups, because of the range of purposes for which data is held. For further details of how theserights are upheld for different groups, please see sections 13-18.

7.3. Individuals may only see information that is held about themselves. Paperwork that also names other individuals should be appropriately redacted to fully protect the privacy of the others.

7.4. Information that individuals may not access includes:

- information about other individuals
- statistics, where persons can be identified
- information which may lead to harm to that individual or another

7.5. Darlington Area Churches Youth Ministry (DACYM) workers should take reasonable steps to ensure that the person making therequest is the person they claim to be.

7.6. As children and young people under the age of 13 years are not considered capable of giving informed consent regarding the use of their personal data, Darlington Area Churches Youth Ministry (DACYM) will also respondto requests from parents if the child in question is below the age of 13. After their 13th birthday, the young person themselves would need to make the request.

8. Acceptable reasons for disclosure of data

8.1. Confidential information may be disclosed in certain circumstances, for example, if disclosure is required by law, or if the disclosure of information is for a particular prescribed purpose relating to Darlington Area Churches Youth Ministry (DACYM) business, or with the consent of the individual
concerned. Express consent is required if sensitive personal data is being processed for the purposes of Darlington Area Churches Youth Ministry (DACYM) business, however if the disclosure relates to actual or possiblefuture legal proceedings then no consent is required. If you are unsure whether you should disclose a piece of information, please contact the Data Controller or Branch Director. (Seealso sections 15 and 16.)

9. Physical data security

9.1. All written printed or hard copy personal data will be kept in a secure lockable cabinet and access will be restricted to those that need access to the information as detailed below.

10. Digital data security

10.1. Darlington Area Churches Youth Ministry (DACYM) uses a range of digital/online data facilities. It is important that all usersensure a proportionate level of security is in place. The following guidelines should be observed:

- Online accounts of any nature should only be accessed by the named holder - users should not share their account access with any other users.
- Passwords should be "strong" when created. Recommended good practice is:
- Make the password at least 12 characters long. The longer the better. Longer passwords are harder for thieves to crack.
- Don't use the same password for everything.

- Include numbers, capital letters and symbols. Consider using a $ instead of an S or a 1 instead of an L, or including an & or %.
- Passwords should be kept secure
  - Do not write on a post-it note on your PC monitor
  - Do not write all of your passwords in one place in your diary or phone.

10.2. Care should be taken not to leave computers or phones unattended when logged onto accounts. Use sleep mode or a password protected screensaver.

10.3. Any phone or tablet device being utilised for Darlington Area Churches Youth Ministry (DACYM) business should be protectedwith password, pin, pattern or other security feature.

10.4. Additional thought and care needs to be taken if any personal data is carried on portable devices such as USB memory sticks. These should be encrypted where possible, and data deleted once it is no longer needed.

11. External contractors and Cloud services

11.1. Darlington Area Churches Youth Ministry (DACYM) will take reasonable steps to ensure that any sub-contractors who hold orprocess data on our behalf are GDPR compliant.

11.2. At present, the organisation uses the following service providers who may hold data on their servers. This list will be updated annually and confirmation sought regarding the compliance of each:

11.3. TBC – need to clarify which we use.Any contractors and consultants employed by Darlington Area Churches Youth Ministry (DACYM)Darlington Area Churches Youth Ministry (DACYM) who have access to data will be asked to confirm that their working practices are GDPR compliant, and that all data will beerased on completion of the work.

11.4. When considering using a new provider or technology, managers must carry out a Data Protection Impact Assessment (DPIA) which should be checked and approved by the Data Controller.

12. Keeping data up to date (including disposal and destruction of data)

12.1. Regulations make it clear that data must only be kept for as long as it is necessary or until the data subject requests its deletion.

12.2. The Data Controller, working with Branch Leaders, will ensure that all data held is up to date and relevant and where these criteria are no longer met, ensure that the data is permanently deleted or destroyed as appropriate.

13. Staff and volunteers

13.1. Personnel files and other confidential staff records will be kept in a locked cabinet for which the line manager, Branch Leader and relevant administrators are the only key-holders.

13.2. All staff will be given a copy of this policy as part of their induction. The implications of the policy for their work will be explained.

13.3. Job application forms, job interview records and job monitoring forms are confidential to Darlington Area Churches Youth Ministry (DACYM). The interview panel will hand in all papers at the end of
interviews. Application forms and records of the selection process will be kept for a period of 1 year; any papers not required for Darlington Area Churches Youth Ministry (DACYM) records will be shredded.

13.4. A privacy notice shall be displayed on all application forms for employees and volunteers explaining what data is kept, for how long, and how they can go about requesting access to it.

13.5. References - When references for new employees are requested, it will be made clear that the references will be available only to the staff member concerned, otherwise they will be confined to the line manager/Branch Leader and members of the interview panel.

13.6. Supervision - With the exception of disciplinary action, information discussed in supervision will be confidential to the people concerned in the meeting and the supervisor's line manager.

13.7. Branch Leaders are responsible for ensuring that all staff adhere to the agreed systems and procedures. This entails being clear about who has access to what information and that filing cabinets and key boxes are locked when rooms are not staffed.

14. Records about young people and other participants

14.1. Records about participants kept under Legitimate Interest will include all those required for Safeguarding and/or Health and Safety purposes, such as project registration forms, attendance registers, session notes/debrief records, referral notes, records of achievements, safeguarding notes and correspondence between Darlington Area Churches Youth Ministry (DACYM) and the participant and/or their family.

14.2. Depending on the nature of the project, data held may include: full name; home address and telephone number; details of and contact information for next of kin; medical information; date of birth; gender; disability; racial/ethnic origin; referral source; type of project engaged in; records of attendance; last date of contact with Darlington Area Churches Youth Ministry (DACYM); length of association with Darlington Area Churches Youth Ministry (DACYM) services; reasons for disengaging; and records of behaviour, participation andachievement.

14.3. Participants' personal data may also be requested for marketing and publicity purposes (e.g. to post information about a special event/residential to youth club members). Consent to use personal data for this purpose will be sought.

14.4. A Privacy Notice shall be displayed on all participant registration forms, which explains what data is kept for Legitimate Interest, for how long, who has access to it and how they can make a request to access it.

14.5. Participants must proactively give informed consent to be added to marketing databases. This will be made clear on all registration forms, with an appropriate Privacy Notice. Children and young people under the age of 13 years are not considered capable of giving informed consent regarding the use of their personal data, so a parent/guardian must give consent for them to be added to marketing databases. Young people aged 13 years and older may give consent on their own behalf.

14.6. Through support and advice work with participants, notes and records may be kept.

If a participant makes a contentious or difficult unsolicited disclosure, staff must make clear that they may need to share information with their Line Manager. In most cases, disclosures should be handled with reference to the relevant safeguarding policy. Where the disclosure is not related to safeguarding, staff may choose not to continue a conversation if they feel that it may be heading to an area of disclosure that they are unhappy to take on board. Wherever possible, consent will be sought to share this information.

14.7. Darlington Area Churches Youth Ministry (DACYM) staff must also treat as confidential all information of a private or personal nature about an individual which they may learn in the course of their duties, and must not communicate this to other persons or bodies, except as indicated in sections 7, 8, 15 and 16.

14.8. Participants will have access to their own files through appointment with their key worker.

14.9. Where staff find themselves in a social setting with participants they work with, or may potentially work with, care needs to be given to ensure that the participants wishes for contact are respected. It should be recognised that in social settings a participant has a right to be anonymous and not attached to a 'project.' Any interaction should maintain confidential.

14.10. Participants taking part in media events must not disclose a project address or names of other participants for public information. Participants will be clearly informed that they are not obliged to take part in any media events if they do not wish to do so.

14.11. The location of project locations will not be disclosed to outside agencies unless there is a legal obligation to do so, or it is in the interest of the participants to do so.

14.12. Visits by external agencies and interested individuals to projects managed by Darlington Area Churches Youth Ministry (DACYM)will be conducted only where appropriate and with participants and staff receiving notification. Such visits will only be allowed when they are essential in assisting the organisation to meet its aims and objectives, or if participants would miss out on an opportunity which would benefit them and in which they have expressed an interest.

14.13. Participants are expected to respect the rights of other participants as regarding the personal information they have about each other. A breach of confidentiality by a participant about another participant may be viewed as harassment and may be cause for a withdrawal of services.

14.14. This policy is to be explained to all participants when it is possible and appropriate to do so, using language which is clear and understandable by them.

14.15. In cases where confidentiality must be broken (see sections 7, 8, 15 and 16), the Branch Leader must be informed and fully involved in the process. Any risk to others should be assessed. Under consultation with the Branch Leader, relevant agencies should be informed.

14.16. Any personal data held on participants for marketing and publicity purposes will be destroyed after 5 years of their last contact with Darlington Area Churches Youth Ministry (DACYM). All records held under Legitimate Interest, including participants' personal data, will be kept secure and retained indefinitely.

15. Data-sharing with statutory bodies, partner agencies and funders

15.1. From time to time it is necessary to share data about participants with other agencies for reporting or referral processes.

15.2. Darlington Area Churches Youth Ministry (DACYM) may give information to other agencies when this has been authorised by a young person. Wherever possible and appropriate, workers should seek permission from participants before sharing data, either when first collecting the information, or in the case of areferral, from the individual before taking the action.

15.3. The staff team will assess when a situation necessitates a breach of confidentiality. The building of a relationship of trust with participants is paramount and confidentiality should normally be maintained, with the following exception:

'Where the participant or another person is deemed by the worker to be at considerable risk themselves or a risk to others.'

In these instances, Darlington Area Churches Youth Ministry (DACYM) may give information to statutory/emergency services e.g.Police, Social Services, Probation or another support agency, even if this is against the expressed will of the participant.

15.4. Social workers and other professional partnership agency staff may disclose sensitive information about participants and their families to Darlington Area Churches Youth Ministry (DACYM) staff. This information isto be treated as entirely confidential and must not be disclosed either to colleagues or workers except in supervision with the Branch Leader.

15.5. When reporting to funders, workers should always seek to anonymise data so that reporting can be completed without individuals' identifiable data being released.

15.6. Where a funder insists on having specific information about participants, we should ensure that all participants are made aware of the transfer and a data-sharing protocol with the funder be established.

15.7. If a third party requests information about present or former participants in general (rather than identified individuals), steps should be taken to ascertain if that information can be disclosed without disclosing the identity of any particular individual. This may be achieved by deleting or editing information so that it becomes anonymised. It will be important to consider if it is reasonable to disclose the information without consent: information should not be disclosed if it is confidential, sensitive or harmful.

16. Participants and criminal activity

16.1. While Darlington Area Churches Youth Ministry (DACYM) would appear to be within its legal rights to refuse to disclose information about participants to the police (unless the person concerned is suspected of committing an arrestable offence), our approach is to offer every reasonable assistance to thepolice in their enquiries.

16.2. In the event of a participant disclosing criminal activity, the worker has to make a judgement about the risk of that activity to the participant and the others in relation to a desire to keep relationships and continued intervention around behaviour and should discuss this at the earliest possible opportunity with the Line Manager/Branch Leader.

16.3. With regard to disclosure to the police, it is an offence to withhold information with regard to criminal activity, should a Darlington Area Churches Youth Ministry (DACYM) worker be asked as part of an official inquiry.

16.4. Steps should be taken to establish the authenticity of a police request by, for example, asking the caller to leave name, rank and station telephone number, and then phoning back and asking for the officer in question.

16.5. In all such cases, workers are encouraged to discuss issues of confidentiality with their line manager/Branch Leader before disclosing personal information about a participant.

17. Marketing, supporters and mailing lists

17.1. Data belonging to individuals will only be held when there is a clear reason for doing so, and only within the Data Protection principles outlined above.

17.2. Individual supporters must be made aware of what data we are keeping, what we intend to do with it, and how they can exercise their "right to be forgotten". This is known as a Privacy Notice.

17.3. Supporters must proactively give informed consent to be added to marketing databases. The organisation must keep records of when consent was given and what Privacy Notice was used.

17.4. Data about supporters will only be held in approved locations, whether online or paper-based records. An inventory of these locations will be held by the Data Controller.

17.5. Darlington Area Churches Youth Ministry (DACYM) respects the privacy of all supporters and with this in mind will never sharepersonal data with individuals or organisations who are not working for the interests of the organisation, unless specific approval is sought beforehand.

18. Board of Trustees

18.1. Board members will be sent a copy of this policy and be expected to implement it in relation to their own papers and information discussed at board meetings.

18.2. All committee papers will be considered confidential and marked 'Private and Confidential.' Board members will take reasonable steps to ensure that papers and communications received by them in connection with their role are secure and kept confidential from colleagues, family and friends.

18.3. References to young people at board meetings will be coded. Young people will not be named.

18.4. Policy reports and incidents will be made in terms of figures only. Specific names or addresses will only be mentioned where absolutely necessary for the Board to make a decision/ judgement.

19. What to do in case of a Data Breach

19.1. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

19.2. Data Breaches also include the potential loss of disclosure of data such as through a lost mobile phone or other device.

19.3. All Data Breaches should be reported at the earliest opportunity to the Data Controller.

19.4. Working with the individuals concerned, the Data Controller will seek to ensure that the data is no longer unsecured and take all reasonable steps to retrieve or ensure destruction of any leaked data.

19.5. The Board appointed Senior Risk Information Officer (SIRO) will then be responsible for overseeing an investigation into the breach, identifying what can be learned to ensure that such a breach does not happen again and assessing whether any disciplinary action is recommended.

19.6. The Data Controller and SIRO will consider the likelihood and severity of any risk to people's rights and freedoms, following the breach. When this assessment has been made, if it is likely there will be a risk, then the Information Commissioners Office must be notified. If the risk is low or unlikely then reporting is not necessary.

20. Training

20.1. Darlington Area Churches Youth Ministry (DACYM) will seek to ensure that all staff and employees are adequately trained tounderstand their obligations with regards to handling personal data.

20.2. It is acknowledged that those with differing levels of responsibility within the organisation will need different training – but everyone, including volunteers, should at least have an awareness of the regulations and responsibilities.

21. In case of doubt

If you have doubts about how to deal with a particular enquiry it should be passed to the Data Controller.

REVIEWED AND ADOPTED – 01/12/2022
NEXT SCHEDULED REVIEW – AUTUMN TERM 2024