Data Protection Policy Dundonald Baptist Church

Under the UK Data Protection Act 2018 and Data Protection and Digital Information (No. 2) Bill we are aware that we have a legal responsibility to handle personal data correctly. This data can include information about members, adherents, employees, volunteers, suppliers, service users and others that we have a relationship with. This policy describes how this personal data must be collected, handled and stored to meet data protection standards that comply with the law.

We have a responsibility to only gather and retain data, which is adequate, relevant and not excessive in relation to the purpose for which it is held and we must have opt in consent to hold and use such data. We must ensure that personal data is accurate and where necessary, kept up to date. We must do what we can to prevent unauthorised or accidental access to personal data and must hold data for no longer than necessary. There is a right to deletion and to be made aware of what data is held.

Policy Scope
This policy applies to Dundonald Baptist Church, to all employees, office-bearers, volunteers, contractors, suppliers and others processing personal data on behalf of the church. It applies to all data that we hold relating to identifiable individuals.

Responsibility
Everyone in the church and who works for us has some responsibility for ensuring how personal data is collected, stored and handled appropriately. In particular the Office-bearers are ultimately responsible for ensuring that legal obligations are met. This includes keeping up to date with current legislation, providing training, reviewing policies and procedures and handling access requests and breaches.

General guidelines
- Training will be given so that everyone is aware of their responsibilities when handling data.
- Data should not be shared informally.
- All reasonable precautions should be taken to keep sensitive data secure.
- Personal data should not be disclosed to unauthorised people both internally and externally.
- Telephone callers identity should be checked before giving out any information and if necessary requesting a written enquiry.
- Data should be regularly reviewed and kept up to date or destroyed securely if no longer required.
- If unsure you can request help and guidance from the office-bearers.
- A privacy policy is made available that details how data relating to the subject is used and their rights including how to raise a complaint.

Collection
- The main legal basis for collecting personal data on our members and those affiliated with us will be on the basis that it is necessary for us to hold said data for the purposes of legitimate interests which are not overridden by the interests of the data subject. In respect of certain types of data and in particular data revealing religious beliefs, this data will be held on the basis that it is processed in the course of the legitimate activities of a not-for-profit religious body and will not be disclosed outside of that body without the consent of the data subject.
- Other legal basis will apply such as employment and contract law and safeguarding.
- Informed consent will be obtained were required informing the data subject of the reasons why the data is required.

Storage
- All data stored on paper, like consent forms, accident forms, or any information on children, Parents, leaders, members, adherents or employees should be kept in a secure, confidential but accessible location. A locked filing cabinet on the premises is a good example. This includes data that is normally held electronically but has been printed for some reason.

- Printed material should not be left lying around unattended.
- All consent forms, accident forms, or any information on children or leaders should only be kept in a person's own possession for the length of time they are absolutely required eg duration of a trip
- Leaders must ensure that they have easy access to relevant data such as children's contact details and medical information when the organisation is meeting.
- Incident/accident forms should also be held securely on the premises.
- Electronic data should be protected from unauthorised access, accidental deletion and malicious hacking attempts. It must be password protected and where possible stored on encrypted devices.
- Electronic data should only be uploaded to an approved cloud-computing platform. The church uses Google Drive.
- All computers holding personal data should have adequate up to date security software and firewall.
- Electronic data should be backed up regularly and held securely.
- It is recognised that due to the nature of the church structure it may be necessary for personal data to be stored on personal laptops and computers. The same policy applies to such equipment and only data that is essential for the running of that organisation is to be used.
- Care should be taken when transferring electronic data that it is encrypted and is destined for the correct person. Avoid sending emails containing data were possible.
- Consideration should be given to make anonymous personal data that is recorded in minutes and personal notebooks eg for visitation.

Access
- Data should only be available on a need-to-know basis.
- The exception to this is certain medical information where it is important that all leaders in a supervisory role are aware of conditions that children in their care have.
- Sensitive data should not be given to any external party but only used for the purpose for which it was given unless required by law or if permission has been obtained eg Payroll, giftaid

Retention
- Data will only be retained for as long as it is required.
- Consent forms should be retained for 1 year and 6 months.
- Attendance rolls kept indefinitely for safeguarding and historical purposes.
- Incident/accident forms 3 years for adults and 3 years after the child reached 18.
- Basic Members details will be retained indefinitely for historical purposes and other data for 3 years after ceasing membership.
- Financial records will be retained for 7 years.
- Application forms 1 year unless employed when it will go in their personnel file and be held until 1 year after the employment ends.

Accuracy
- Everyone will take reasonable steps to ensure the accuracy of information held.
- Data will be held in as few places as possible and should not be needlessly duplicated.
- Regular attempts to confirm the accuracy of the data held will be made. Normally annually.

Disposal
- Printed copies of data that are no longer required should be shredded using a cross shredder.
- Electronic data that is no longer required should be permanently erased.

Subject Access Requests
- Individuals have the right to request to access the personal data that an organisation holds on them. This must be provided free within 40 days of the request, which can be received by anyone and in any form. All such requests should be brought to the attention of the office-bearers as soon as possible.
- Care will be taken to ensure the person is who they say they are before the data is released.

Security Breach
Despite the precautions taken data may still be lost or accessed inappropriately. This may occur through …

- Loss or theft of data or equipment
- People gaining inappropriate access
- A deliberate cyber attack or malicious virus
- Equipment failure
- Human error
- Catastrophic events like fire or flood

In such cases the office-bearers should be informed immediately. They will investigate the breach to find the cause and scope and judge if there is risk of harm resulting from it. If it is considered that there is a risk of harm the ICO will be informed within 72 hours. Those affected will be informed without delay. If necessary, the church insurers, solicitors and police will be informed. Steps will be taken to mitigate the risk and prevent the breach from reoccurring.

Review
This policy will be reviewed annually by the office-bearers.
Last reviewed 2-10-2023 David Morrow (Elder)