

DBN DATA PROTECTION POLICY

1.06.2018

This Policy has been approved by DBN General Assembly on the 1st of June 2018

1. Introduction

Don Bosco Network needs to gather and use certain information about individuals and organizations. These can include: employees, volunteers, DBN members, partners, beneficiaries and other people the organization has a relationship with or may need to contact. This personal and confidential information must be collected and dealt with appropriately whether is collected on paper, stored in a computer database, or recorded on other material and there are safeguards to ensure this under current data protection legislation. This Policy describes how this personal and organization data must be collected, handled and stored to meet the organization data protection standards and to comply with the European Union and Italian law as Don Bosco Network is a registered Association in Italy in accordance with Italian law.

This data protection policy ensures that Don Bosco Network:

- Complies with data protection laws and follow good practice
- Protects the rights of staff, volunteers, beneficiaries and partners
- Is open about how it stores and processes individual's and organizations' data
- Protects itself from the risks of data breach (data breach will be reported to relevant authority within 72 hours)

2. Data protection law

Don Bosco Network policy is compliant to European Union (GDPR 2018) and Italian data protection legislation which is based on following principles when processing personal data:

- 1) lawfulness, fairness and transparency;
- 2) purpose limitation;
- 3) data minimisation;
- 4) accuracy;
- 5) storage limitation; and
- 6) integrity and confidentiality

3. People, risks, and responsibilities

This policy applies to all Don Bosco Network employees and volunteers in regards to all personal data information stored and processed by Don Bosco Network. This policy applies to employees and volunteers of Don Bosco Network members and partners in regards to sharing information on Don Bosco Network online platform.

This Policy helps to protect Don Bosco Network from some real security risks, including:

- **Breaches of confidentiality.** For instance, information given out inappropriately.
- **Falling to offer choice.** For instance, all individuals will be free to choose how the organization uses data relating to them.
- **Reputational damage.** For instance, the organization could suffer if hackers successfully gained access to sensitive data.

Responsibilities:

Everyone who works for or with Don Bosco Network has some responsibility for ensuring that data is collected, stored and handled appropriately. Everyone that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. The following people have key areas of responsibility:

- **Data Controller** - The Board is ultimately responsible for ensuring that Don Bosco Network meets its legal obligation
- **Data Protection Officer (*VIS designated person*)** is responsible for:
 - Keeping the Board updated about the data protection responsibilities risks and issues.
 - Reviewing all data protection procedures and related policies in line with the agreed schedule.
 - Handling data protection questions from staff and anyone else covered by this policy.
 - Checking and approving any contracts or agreements with third parties that may handle the organization sensitive data.
 - Reporting data breach to Italian Data Protection Authority within 72 hours
- **DBN Secretary (*currently Network Coordinator*)** is responsible for:
 - Ensuring all systems, archives cabinets, services and equipment used for storing data meet acceptable security standards.
 - Performing regular checks and scans to ensure security hardware and software is functioning properly.
 - Evaluating any third-party services the organization is considering using to store or process the data.
 - Answering any data protection queries from partners and media.

- Dealing with individuals to see the data Don Bosco Network holds about them.
- Investigating instances of breach and informing immediately the Board and DBN President.
- If the breach is likely to result in a high risk to the rights and freedoms of individuals, DBN Secretary will notify the individuals affected.

4. General guidelines

- The only people able to access data covered by this policy will be those who need it for their work
- Data should not be shared informally. When access to confidential information is required it can be requested from the responsible personnel.
- Employees and volunteers should keep all data secure, by taking sensible precautions and following the guideline below.
- In particular strong passwords must be used and they will never be shared.
- Personal data will not be disclosed to unauthorised people either within the organization or externally.
- Data will be regularly reviewed and updated. If it is no longer required it will be deleted and disposed of.
- Staff and volunteers will request help from the DBN Secretary if they are unsure about any aspect of data protection.

5. Data collection

Don Bosco Network will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, Don Bosco Network will ensure that the Individual/Service User:

- Clearly understands why the information is needed
- Understands what it will be used for
- As far as reasonably possible, grants free explicit consent, either written or verbal for data to be processed
- Has received sufficient information on why their data is needed and how it will be used

6. Data storage

The rules below describe how and where data and confidential informations of Don Bosco Network, Network members and partners will be safely stored. Questions about storing data and confidential information safely can be directed to DBN Secretary.

When data is stored on paper, it will be kept in a secure place when unauthorised person cannot see it.

- When not required, the paper or files will be kept in the locked drawer or filing cabinet.

- Staff and volunteers will make sure that printouts are not left where unauthorised people could see them.
- Data printouts will be shredded and disposed of securely when no longer required
- When data is stored electronically it must be protected from unauthorised access, accidental deletions and malicious hacking attempts.
- Data will be protected by strong passwords that are changed regularly
- Data stored on removable media will be kept locked away securely when not being used.
- Data will be stored only on designated drives and servers and will only be uploaded to an approved Cloud computing service.
- Data will be backed up frequently.
- All servers and computers containing data will be protected by approved security software and a firewall.

7. Data usage and accuracy

Personal data and confidential information is used by Don Bosco Network responsibly. All Individuals/Service Users have the right to access the information Don Bosco Network holds about them. Don Bosco Network will also take reasonable steps to ensure that this information is kept up to date by asking data subjects whether there have been any changes.

In addition, Don Bosco Network will ensure that:

- Everyone processing personal and confidential information understands that they are contractually responsible for following good data protection practice
- Everyone processing personal and confidential information is appropriately trained to do so
- Anybody wanting to make enquiries about handling personal information knows what to do
- It deals promptly and courteously with any enquiries about handling personal information
- It will regularly review this policy and audit the ways it holds, manage and use personal and confidential information

8. Security provisions for the DBN online platform

Don Bosco Network in agreement with Don Bosco Network members and partners worldwide provides online platform at the service of the network members and partners to support effectiveness in their work. The online platform is fully compliant with EU and Italian data protection legislation. Personal contact details of staff and volunteers of network members and partners are shared through online platform internationally, outside of the EEA only with the registered users of the platform and with the consent of the data subject. You will find below safety provisions assuring security and data protection of the online platform:

- Don Bosco Network online platform is fully integrated with the website: www.donbosconetwork.org



- The Board of Don Bosco Network has final decision on the content of the platform and granting access to the platform or parts of it through various levels users accounts according to the internal agreement between network members and partners on website users levels.
- Don Bosco Network Secretary/Coordinator executes day to day administration of the Platform and assures online security for personal data and confidential information of the Don Bosco Network members, partners and all the platform users. He/she will remind all platform users on regular changing of personal passwords.
- IT company contracted to build and service the platform is obliged to data protection EU legislation and confidentiality under signed contract.
- Projects data base is updated 2 times a year according to the agreed template. The projects can be send by DBN members and partners in a provided format to DBN Secretary/Coordinator for upload or appointed person in particular organization can upload them directly to the website in agreement with DBN Secretary/Coordinator. Full access to the information about projects is password protected and available only after user login to the platform.
- All documents and materials in Own Cloud resources are password protected and available only after user login to the platform. Materials which are outdated or are not in use anymore will be removed from the resources.
- Volunteers data base is available for viewing only to website users after login. DBN provides information about placement of currently serving volunteers of network members and partners to help coordinate their work on the ground. Once volunteer finishes placement information about his/her placement will be removed from the platform.
- PDO platform fully integrated with DBN website is an online capacity building tool. Documents and detailed information about PDOs are available only after login to the platform. This information is constantly updated by DBN Secretary/Coordinator. Outdated information and materials will be removed from the platform.
- DBN members and partners using the online platform are obliged to inform DBN secretary of relevant personnel changes. Personal users account and information about old staff will be removed from the online platform once the DBN Secretary receives information about the change.