DATA PROTECTION POLICY

eVidyaloka Trust, Bengaluru

June 2018

Rev 0

Definitions

Charity	means eVidyaloka, a registered charity.
GDPR	means the General Data Protection Regulation.
Responsible Person	Means Mr. Venkat Sriraman
Register of Systems	Means a register of all systems or contexts in which personal data is processed by the Charity.

1. Data protection principles

The Charity is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

2. General provisions

a. This policy, jointly with the Privacy Statement (Exhibit 1) applies to all personal data collected/processed by the Charity.

b. The Responsible Person shall take responsibility for the Charity's ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.

d. The table below shows the confidentiality and consent tie-ups in eVidyaloka.

	Consent	Agreement
Volunteers	XX	XX
Donors Individual	XX	Optional as required
Donors Corporate	----	XX
Employees	------	XX
Partners	----	XX
Schools		
Students		
Account/IT/Data Storage contractors	-----	XX

3. Rationale

eVidyaloka needs to process certain information about its staff, volunteers, NGO partners, students and schools, donors and other individuals with whom it has a relationship for various purposes such as, but not limited to:

1. The recruitment and payment of staff.
2. The administration of programmes of study and courses.
3. School/class enrolment.
4. Examinations and assessment.
5. Recording student progress, attendance and conduct.
6. Complying with obligations to funding bodies and government

To comply with various legal obligations, including the obligations imposed on it by the General Data Protection Regulation (GDPR) eVidyaloka must ensure that all this information about individuals/organisations is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

4. Compliance

This policy applies to all staff of eVidyaloka. Any breach of this policy or of the Regulation itself will be considered an offence and the Charity's disciplinary procedures will be invoked.
As a matter of best practice, other agencies and individuals working with Charity and who have access to personal information, will be expected to read and comply with this policy. It is expected that departments who are responsible for dealing with external bodies will take the responsibility for ensuring that such bodies sign a contract which among other things will include an agreement to abide by this policy.

5. Responsibilities under the GDPR

The 'top/senior management' is responsible for all day-to-day data protection matters, and will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling within the Charity.
Compliance with the legislation is the personal responsibility of all members of the Charity who process personal information.
Individuals who provide personal data to the Charity are responsible for ensuring that the information is accurate and up-to-date.

6. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the Charity shall maintain a Register of Systems.
b. The Register of Systems shall be reviewed at least annually.
c. Individuals have the right to access their personal data and any ~~such~~ requests made to the charity shall be dealt with in a timely manner.

7. Lawful purposes

a. All data processed by the charity must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests.
b. The Charity shall note the appropriate lawful basis in the Register of Systems.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Charity's systems.

8. Data minimisation

The Charity shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

9. Accuracy

a. The Charity shall take reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

10. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, the Charity shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
b. The archiving policy shall consider what data should/must be retained, for how long, and why.

11. Security

a. The Charity shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
c. When personal data is deleted this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.

12. Implementation and dissemination

Regularly offer staff training on practical data protection issues like clearing out old information, keeping their access passwords secure, etc.

Also there is a staff and system in place to attend to the requests received from any of the stakeholders.

13. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Charity shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach.

Signed:

Date:

Register of Systems

Stakeholders: eVidyaloka/staff/Volunteers/NGO partners/Donors/Schools/Students/Contractors
It is our policy and commitment that we minimise data collection and processing, restricting the same to 'essential'.
Data are shared essentially for the regular functioning, for example about students with the volunteer teachers and/or about the volunteers with the coordinators in the school site. Personal data are not otherwise collected or shared.
Data except those of employees are collected and stored digitally. The storage in a server is augmented with a disaster recovery plan by the storage provider and privacy agreement is in place.
Accounting services are outsourced for the Trust. We have a data protection and confidentiality commitment from them.
Data is shared internally only as required and except for compliance purposes there is minimal processing done. The access to data is limited to those who need it for operational purposes.
Any exception to this policy based on situational requirement is authorized by top management officers Venkat and Manohar.

The following is the tabulation of the data storage, processing and security arrangements by us.

S. No	Role	Data	Access	Location	Process	Security measures
1	Employees	Name, number, email address, residence address, photo	Admin, HR, Venkat, Accounts Team	Hard Copies in a box fileSoft copies in mail accounts of Venkat, interviewing panel	Salary creditReview meetingsMedical InsuranceI card generation	1. Soft and hard data under controlled access. 2. Access register reviewed every year. 3. Access withdrawn for exiting staff including volunteers/interns
2	Volunteers	Name, Number, email address	VM, Ops, Management Team, Content Team, Other employees of eV with admin access, Interns, FC, CA	Volunteer Dashboard Backend Admin page Server Downloaded excels in employee desktops One Drive folders Attachments in emails Google Drive	Analysis Volunteer Dashboard Offerings Report Back end (Django) Server Downloaded excels in employee desktops One Drive folders Attachments in emails Google Drive	1. Soft and hard data under controlled access. 2. Training for staff. 3. Confidentiality agreements with those with whom we share data for operational purposes. 4. Access withdrawn for exiting staff including volunteers/interns. 5. Extra care when data used for mass communication.

3	Partner	Name, Number, email address	Ops, Volunteer Teachers, CA, other employees of eV with admin access	Volunteer Dashboard Center Page Backend Admin page Server One Drive folders Attachments in emails Google Drive	Analysis Volunteer Dashboard Back end (Django) Server Downloaded excels in employee desktops	1. Soft and hard data under controlled access. 2. Training for staff. 3. Confidentiality agreements with those with whom we share data for operational purposes. 4. Access withdrawn for exiting staff including volunteers/interns
S. No	**Role**	**Data**	**Access**	**Location**	**Process**	**Security measures**
4	School and HM	Address, Phone number	Ops, Admin, FC, CA	Center Page in Jupiter School Identification Template Anyone interested to visit school	Infra Purchase Infra Maintenance Internet Bill payment Infra Audit Field visit	1. Soft and hard data under controlled access. 2. Training for staff. 3. Confidentiality agreements with those with whom we share data for operational purposes. 4. Access withdrawn for exiting staff including volunteers/interns
5	Students	Name, Photo	Ops team, CA, Volunteer Teachers, FC, PA, other employees of eV with admin access	My Students page in Jupiter Server One Drive folder Ops team mails/ desktops	Students Dashboard Server Back end (Django)	1. Soft and hard data under controlled access. 2. Training for staff. 3. Confidentiality agreements with those with whom we share data for operational purposes. 4. Access withdrawn for exiting staff including volunteers/interns. 5. Extra care when data used for mass communication.

6	Donors Individual	Name, Phone number, email id	Ops team, Employees of eV with Admin login	Server , One drive folder	Tagging their sponsored schools	1. Soft and hard data under controlled access. 2. Access register reviewed every year. 3. Access withdrawn for exiting staff including volunteers/interns
7	Donor Corporate	Name, Phone number, email id	Ops team, Employees of eV with Admin login	Server , One drive folder	Tagging their sponsored schools	1. Soft and hard data under controlled access. 2. Access register reviewed every year. 3. Access withdrawn for exiting staff including volunteers/interns