Adopted by board of trustees……

Signed…….

Data Protection Policy
Written: May 2018
Published: May 2018
Review: May 2019

DATA PROTECTION POLICY

Purpose

Dame Vera Lynn Children's Charity (DVLCC) has a system which upholds the importance of privacy for the individual, whether it be a child, adult, member of staff, parent or member of the community and this sets out our commitment to data protection.
As a Data Controller (DVLCC) is required to maintain certain personal data about individuals for the purpose of satisfying operational and legal obligations. The types of personal data that DVLCC may require include information about current, past and prospective employees, Charity trustees, governors and donors, suppliers and young people who use the DVLCC's services. This personal data, whether it is held on paper, on computer or other media, will be subject to the appropriate legal safeguards as specified in the Data Protection Act 2018. DVLCC has registered its use of personal data to the Information Commissioners Office as required under the Act. Our Data Protection Registration Number is Z9711470.

Equality Impact

This policy will ensure that confidential data about all stakeholders held securely and only shared internally where there is need and externally where there is a clear, legal requirement to do so.
At DVLCC the arrangements for protecting the privacy of clients and staff shall not prevent the sharing of data that needs to be shared and that damage that might result from not sharing information.
In particular requirements under Safeguarding regulations must be adhered to.

RESPONSIBILITIES

DVLCC fully endorses, and adheres to the seven principles of the Data Protection Act 2018. Employees and any others who obtain, handle, process, transport and store personal data for DVLCC must adhere to these principles.

The **seven principles** require that personal data shall:

- Be processed fairly and lawfully. Consent must be kept separate and distinct from other terms and conditions. It must be freely given, specific, informed and unambiguous. As easy to withdraw as to give (and can be withdrawn at any time)
- Be obtained only if it is needed for a specific purpose.
- Be limited to what is actually needed and not be excessive.
- Be accurate and up-to-date at all times.
- Not be kept any longer than necessary.
- Be treated with integrity and remain confidential within the organisation. Data will be kept securely online and paper copies held in a secure locked area.
- We will demonstrate compliance with data protection principles. Keeping a detailed record of processing operations. Performing data protection impact assessments for high risk processing. Designating a data protection officer if necessary. Notifying and recording data breaches. Implementing data protection by design and default.

DVLCC is responsible for ensuring its compliance with the Data Protection Act. All staff are responsible for the implementation of this Policy. All staff must be made aware of the principles of the Act and attend any necessary training. It is the responsibility of managers to remind staff of Data Protection requirements as appropriate and to ensure that staff have attended data protection training as required. Any breach of this policy should be reported immediately to the Executive Manager.

PROCESSING IN LINE WITH DATA SUBJECTS RIGHTS

Data must be processed in line with data subject's rights. Data subjects have a right to:

- Request access to any data held about them by DVLCC.
- Prevent the processing of their data for direct-marketing purposes.
- Ask to have inaccurate data amended.
- Prevent processing that is likely to cause damage or distress to themselves or anyone else.
- Any correspondence concerning a data subject's rights received by a member of staff must be in writing and should be forwarded to the Executive Manager.
- A formal request from a data subject for information that is held about them must be made in writing. Any member of staff who receives a request relating to access to personal information should request that it be put in writing. The request should then be forwarded immediately to the Executive Manager. The request must be acknowledged and information provided within 40 calendar days.

DATA SECURITY

Appropriate security measures must be taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

The Data Protection Act requires procedures and technologies to be put in place to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if they agree to comply with our procedures and policies, or if they put in place adequate measures themselves.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that only people who are authorised to use the data can access it.
- Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored securely on the central computer system and not on individual PCs.

The level of security required will be dependent upon the sensitivity of the personal data and the risk of it being compromised. As a minimum, security procedures should include consideration of the following:

- Entry controls. Ensure that staff are aware of any visitors that are due to be visiting the Centre and ensure that a member of staff is available to meet and greet anyone that enters the reception area.
- Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential)
- Methods of disposal. Paper documents should be shredded and held in a secure confidential waste bag to be disposed of and not put into the general waste.
- Digital media should be physically destroyed when no longer required.
- Equipment. Data users should ensure that individual monitors do not show confidential information to any visitors and that they log off from their PC when it is left unattended.
- Encryption. Where it is necessary to transfer sensitive personal data by way of a portable device or via email, such information should be encrypted.

PROVIDING INFORMATION OVER THE TELEPHONE

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information. In particular they should:

- Check the caller's identity to make sure that information is only given to a person who is entitled to it.
- Suggest that the caller put their request in writing if uncertain about the caller's identity or if their identity cannot be checked.
- Refer to the Executive Manager for assistance. No-one should be bullied into disclosing personal information.
- Where providing information to a third-party, do so in accordance with the eight data protection principles.

ENSURING PROTECTION OF PERSONAL DATA – PRIVACY IMPACT ASSESSMENTS

A Privacy Impact Assessment (PIA) must be considered whenever there is a change to the way that data is processed, whenever new activities are performed, or at the start of any project where personal information may be processed. Guidance on conducting PIA is available from the ICO. Conducting a PIA ensures that any new risks are identified and suitable controls put in place to ensure the on-going protection of personal data.

ARRANGEMENTS FOR MONITORING AND EVALUATION

The Executive Manager should arrange for an annual audit report, indicating how DVLCC complies with each of the enforceable principles in the Data Protection Act 2018.