Data Protection Policy

Policy Information	
Organisation / data controller	The Boys' Brigade
Scope of the policy	This policy applies to paid staff, trustees, volunteers and anyone acting on behalf of The Boys' Brigade
Policy written by:	Jonathan Eales, Business Director
Policy approval date:	Agreed by the Brigade Executive on 6th June 2015
Policy review date:	June 2016

Introduction

The purpose of this policy is to enable The Boys' Brigade to:

- comply with the law in respect of the data it holds about individuals;
- follow good practice;
- protect staff, volunteers, young people and other individuals, by respecting their rights;
- demonstrate an open and honest approach to personal data; and
- protects the organisation from the consequences of a breach of its responsibilities.

This policy applies to all the information that we control and process, relating to identifiable, living individuals including electronic and paper based records.

The Boys' Brigade recognises a duty under the Data Protection Act to:

- keep information securely and in the right hands;
- to hold good quality (accurate and up-to-date) information;
- only to process relevant information and to do so in accordance with the rights of the individual;
- not keep information longer than is necessary.

Data Storage and processing

The Boys' Brigade recognises that data is held about:

- Staff
- Trustees
- Volunteers
- Young People

This information is always stored securely and access is restricted to those who have a legitimate need to know. As an organisation we are committed to ensuring that all those whom we stored data about understand how and why we keep that data, and how may have access to it.

Retention of Data

Archived records are stored securely and The Boys' Brigade has clear guidelines for the retention of information. See attached appendix.

Roles / Responsibilities:

The Trustees recognises its overall responsibility for ensuring that The Boys' Brigade complies with its legal obligations. The Data Protection Officer is currently the Business Director, with the following responsibilities:

- Briefing trustees on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising other staff on Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Notification *(where appropriate)*
- Handling subject access requests

All staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their roles.

Significant breaches of this policy will be handled under The Boys' Brigade's disciplinary procedures.

Where anyone within The Boys' Brigade feels that it would be appropriate to disclose information in a way contrary to the confidentiality policy, or where an official disclosure request is received, this will only be done with the authorisation of the Data Protection Officer. All such disclosures will be documented.

Key risks to the safety of the data we control and process

The Boys' Brigade has identified the following potential key risks:

- Breach of confidentiality (information being given out inappropriately);
- Individuals being insufficiently informed about the use of their data;
- Misuse of personal information by staff or volunteers;
- Failure to up-date records promptly;
- poor IT security;
- direct, or indirect, inadvertent, or deliberate unauthorised access;
- security of Information held offsite by staff, trustees and volunteers;

The Boys' Brigade will regularly review its procedures for ensuring that its records remain accurate and consistent and, in particular:

- IT systems will be designed, where possible, to encourage and facilitate the entry of accurate data;
- Data on any individual will be held in as few places as necessary, and all staff and volunteers will be discouraged from establishing unnecessary additional data sets;
- Effective procedures will be in place so that all relevant systems are updated when information about any individual changes;
- Training will provided to all relevant staff where required and the Data Protection Officer will monitor data security;

If a breach of data security is suspected or occurs, the Data Protection Officer should be notified immediately.

Access:

Access to personal data and sensitive personal data is restricted to those who have a legitimate requirement for access.

Any subject access requests will be handled by the Data Protection Officer. Subject access requests must be in writing. All staff and volunteers are required to pass on anything which might be a subject access request to the Data Protection Officer without delay. Where the individual making a subject access request is not personally known to the Data Protection Officer their identity will be verified before handing over any information.

An administration charge may be made to persons requesting access to data.

More information:

Full information about the Data Protection Act, its principles and definitions can be found at www.ico.gov.uk

If you have a complaint about the manner in which we have processed your personal data, or receive a complaint from another please contact the Business Director (Data Protection Officer).

Appendix – Retention of data schedule

TYPE OF DATA	GUIDELINE RETENTION PERIOD
EMPLOYEE RECORDS	
Accident Reports	Three years after last entry or end of investigation if later
Staff personnel records	Six years after employment ceases
Details of references	Duration of employment
Wages, expenses and overtime records	Six years plus the current year
Records of unsuccessful applicants, including references	Six months after notifying the unsuccessful candidate
Statutory Maternity Pay records	Six years after employment has ceased
Sickness Records	Six years after employment has ceased
Payroll documentation	Six years after employment has ceased
Pension records	Three years after the end of each tax year for Statutory Sick Pay purposes
Details of Disclosure checks	In accordance with DBS, PVG, Garda Vetting and Access NI Code of Practice
VOLUNTEER RECORDS (including Trustees)	Indefinitely for historical and statistical purposes
Details of Disclosure checks	In accordance with DBS, PVG, Garda Vetting and Access NI Code of Practice