Buckingham Youth Clubs Ltd

CONFIDENTIALITY POLICY AND DATA MANAGEMENT POLICY

The Management Committee of Buckingham Youth Clubs Ltd believes that the welfare of a young person is paramount and that both leaders and young people have a right to expect personal information to be treated as confidential and kept secure. Breaches of confidentiality are treated seriously. However, in certain circumstances, information received in confidence may need to be shared with the appropriate authority to ensure best care for the individual.

Information will always be treated with the utmost confidence and not divulged outside the club apart from the exceptions that follow, which **may** be shared on a "need to know" basis in the following circumstances:

- If the young person is under 18 and physical, sexual or emotional abuse is suspected
- If a young person under 18 reports or alleges abuse
- If the life of the young person or another is at risk
- If information is revealed about criminal activity
- If a young person could cause harm to themselves or others
- If a club leader has reasonable cause to believe a young person is suffering or likely to suffer significant harm

Personal data relating to leaders and young people should be kept secure. This means information relating to an individual from which they can be identified.

If an adult or young person leaves the club all records relating to him will be kept for a maximum of five years and then destroyed.

The management committee will make sure its policy meets the requirements of the Data Protection Act, Rehabilitation of Offenders Act and Children's' Acts.

Staff will be made aware of the policy at induction and understand they are bound by confidentiality.

Paid staff, volunteer staff and the management committee will not discuss a young person with anyone who does not work in the club.

This policy was first adopted by the Management Committee April 2012

On behalf of the Management Committee: (signed)……..
This policy will be reviewed annually by the Management Committee
(Action4Youth will inform all clubs of changes to existing legislation)

DATA MANAGEMENT POLICY

Introduction

Buckingham Youth Clubs Ltd are legally required to conform to the:

- The Data Protection Act [DPA] 1998 - governs the collection, recording, storage, use and disclosure of personal data, whether such data is held electronically or in manual form. Young people have the same rights as adults under the Act;
- General Data Protection Regulations 2018 - The EU's General Data Protection Regulation [GDPR] raises the standards for processing personal data, to strengthen and unify protection for individuals across the EU. This is a result of the changes in our lives, mainly due to the internet. The new legislation comes into force in the UK on 25 May 2018 and will exist post-Brexit;

BYC's have the following policies in place:

1. Safeguarding Policy 2018 - This policy details . . .
    a. *"Leaders will not give out personal numbers and email addresses and will not have young people on their personal social networking sites."*
    b. *Leaders should not "Keep young peoples personal data (photographs and phone numbers/texts/emails) on their personal mobile phones or computers."*
    c. *"Photos should not be stored on personal computers, laptops, tablets, mobile phones or memory sticks."*

2. Confidentiality Policy 2011 - This policy details . . .
    that data "should be kept secure. This means information relating to an individual from which they can be identified.
    If an adult or young person leaves the club all records relating to him will be kept for a maximum of five years and then destroyed.
    The management committee will make sure its policy meets the requirements of the Data Protection Act, Rehabilitation of Offenders Act and Children's' Acts.

This document explains the implications of the DPA and the GDPR for BYC and implements new Data Handling Policies to compliment and replaces aspects of the two existing policies to update BYC's operating procedures .

Background

What is Data Protection ?

Data protection and the DPA governs the right of a person to privacy by the way their data is obtained, stored and used. To do this there are laws and obligation for BYC to follow.

All data obtained is covered by the laws but special focus should be on computer or automated records

(including email and attachments) especially where there is specific information about a particular individual that can easily be retrieved e.g. manual records filed by the name or role etc.

Examples of include:

- Computer files (inc. emails), stored on hard drive, USB stick, and cloud based;
- Images and video
- Files on members, volunteers and young people;
- Indexes of members, including consent forms;

Mention a person is not personal data, eg to say they attended a session, however if the person is specifically discussed or recorded in notes and such identifiable in the record then this does become personal.

What is personal data ?

Data that could be used to identify a living person.

This may be documentation but can also images, video or sound recordings.
There are special rules for Sensitive Personal Data and extra care must be taken. Data becomes sensitive if it includes information about:

1. Racial or ethnic origin;
2. Political opinions;
3. Religious beliefs;
4. Trade union membership;
5. Physical or mental health; or
6. Sexual life;
7. Commission of offences or alleged offences.

What are the rules?

There are 8 basic principles of data management, taken from the Information Commissioner's Office, highlighted in bold

1. *Personal **data shall be processed fairly and lawfully** and, in particular, shall not be processed unless –*
    a. *at least one of the conditions in Schedule 2 is met, and*
    b. *in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.*
2. *Personal data **shall be obtained only for one or more specified and lawful purposes**, and **shall not be further processed** in any manner incompatible with that purpose or those purposes.*
3. *Personal **data shall be adequate, relevant and not excessive** in relation to the purpose or purposes for which they are processed.*

4. *Personal **data shall be accurate and, where necessary, kept up to date**.*
5. *Personal data processed for any purpose or purposes sh**all not be kept for longer than is necessary for that purpose** or those purposes.*
6. *Personal data shall be processed in accordance with the rights of data subjects under this Act.*
7. ***Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.***
8. *Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.*

What is 'Processing'?

Includes all aspects of handling data

- Obtaining;
- Recording;
- Filing / retaining;
- Sharing;
- Deleting / shredding

What is a Data Controller?

A nominated person, or group of people organisation, who are responsible for the compliance of the law, including DPA

There can be a Data Protection Officer (DPO) to ensure compliance but it is the Data Controller (DC) who remains responsible.
POLICY

Terms and Definitions

1. Data Controller - At the time of publishing this is **Katie Cleminson**
2. Person - The subject of the data
3. Staff - Those that are under contract with Buckingham Youth Centre
4. Volunteers - Those that are work with Buckingham Youth Centre and may be given access to data held;
5. Shall - A rule to be followed without deviation
6. Should - A rule that as a preference should be followed, although deviation may be permissible;

Data Held

Includes, but not limited to :

- Membership forms;

- Recorded incident forms;
    - Including accidents;
- Registers;
- Trip Forms, including consent;
- Staff files;
- Complaints;

Data Acquisition

Applicable to all Staff & Volunteers.

Policy

1. All digital data shall be input directly into a managed G Suite product;
2. Data should be directly by the Person,
    a. This is especially true is the data falls within the 7 special categories discussed in What is personal data ? section;
    b. This may be through the use of a online form;

Process

1. Ensure that there is a reason as to why you are collecting the data;
2. Explain why you are collecting the data and who it may be shared with when you collect it;
3. Ensure that you have consent from the individual, this can just be a statement before they sign it (with a pen or with a tick on a box)
4. Before collecting the data ensure that you are familiar with the:
    a. The storage policy in Data Storage Locations section of this document and plan how you are going to store it;
    b. Review the retention needs for the data as the policy in Data Retention Policy;
5. Were possible data should be acquired through the following means:
    a. Through a Buckingham YC G Suite product, this could be
        i. Forms;
        ii. Sheets;
        iii. Docs;
    b. Buckingham YC G Suite Sheets;
6. Where needed, paper documents shall be produced, however the Data Controller must be informed;
7. If you are receiving sensitive data from a third part, you need to consider steps 1-4;

Data Storage Locations

Policy

1. Data shall not be shared, digitally or in hard format, unless permission has been granted;

a. Eg medical information on consent forms can only be shared when permission is granted.

2. Digital data shall be stored using Buckingham G Suite accounts. This is in preference to paper;
3. Digital data should be stored using Buckingham G Suite Team Drives, rather than local drives;;
4. Access to Team Drives will be dependant upon the role of the staff and volunteer;
5. Buckingham Youth Centre hold data in hard format and where this is the case access shall be controlled through the use of secure cabinets;

Security

1. All staff requiring access or generating data or use of the document systems shall
    a. only use a Buckingham YC's G Suite system;
    b. be provided an individual log in to the Buckingham YCs G Suite system;
        i. Buckingham YC have adopted G Suite as it's principle means of digital data storage and data management;
        ii. G Suite is significantly different to a Personal use Google account with policy control that fulfills the DPA requirements;
    2. Staff are permitted to sign into their G Suite account from any device;
    a. This may require the installation of Policy Management software;
3. Staff shall only save data to the local drives on BYC issued computers;
4. Staff must not share their login in details allowing the use of an issued G Suite account to another person to gain access to data shall be considered grounds to disciplinary;
5. An individual's access through the G Suite account shall be removed upon the termination of employment or volunteering this will be;
6. Data generation and exchange should be using the following:
    a. Phone calls;
    b. G Suite GMail;
    c. G Suite Apps;
        i. Docs;
        ii. Sheets;
        iii. Forms etc
    d. Whatsapp;
        i. Note this will require Staff and Volunteers to be happy to share their mobile number;

Data Retention Policy

Policy

1. All stored data shall be sorted into type and year;
2. Data retention shall be reviewed on a period basis, this is as thr following table:

Process

The following act as guidelines:

Document Type	Location	Duration	Notes
Email	G Suite/ ….	2 years	Any personal data i.e. CVs, Appraisals, emails to be stored in Office documents.
Invoices	Office/ Hirers/ Invoices	7 years	To cover at least 1 FY, though may be required for up to 7 years
Application forms	Office/ Staff/ Recruitment	6 Months after employment ends	
Staff Time Sheets	Office / Timesheets / YEAR	2 years	To cover at least 1 FY, though may be required for up to 7 years
Staff Recruitment Inc CVs, References and Interview Notes	Office / Staff / Recruitment	- After interview / shortlisting OR - End of probation period	Scoring of successful staff can be copied into staff appraisal
Annual Membership Forms	Secure cabinet (Existing paper forms) Office / Membership forms (Online forms)	3 years	
Complaints	Secure cabinet	5 years OR Until the person mentioned is 21	

Web Policy

- Buckinghamyc.org.uk is the principle website for Buckingham Youth Club Ltd;
- All Buckingham Youth Club social media accounts shall not contain any of the sensitive data, nor images relating to any members;

Policy

1. buckinghamyc.org.uk will collect anonymised user data through the use of cookies;
    a. Cookies will be retained for 24 months and automatically deleted;
    b. User-ID shall not be used;
    c. Remarketing of User data shall not be used;
    d. Advertising Reporting Features shall not be used;

Appendix 1 - Introduction to G Suites

Online training is available here :
https://gsuite.google.com/learning-center/