

BCLC Data Protection Policy

Summary – Who we are:

BCLC is a not-for-profit church based excepted charity. The church was founded nearly 90 years ago, being constituted with a Trust Deed in 1943. Since then the church has developed and in 2004 the name of the church was changed to Bethlehem Church Life Centre. In 2005 we opened a new multi-purpose building which is specifically designed to be community relevant with many community focussed facilities, programmes and activities operating from the new building including a new Gym, which was opened in April 2008.

General Statement:

As a Church Based Charity and a Not-For-Profit Organisation we consider that we comply with the Data Protection Act Exemption From Notification For Not-For-Profit Organisations, but we endeavour to treat all the information that we store to comply with the Data Protection Act Good Practice Guidelines For The Protection Of Personal Information.

The Information That We Hold:

1. Sensitivity

We hold membership information on various digital databases for Church membership, Children and Youth membership and Gym membership.

We consider that the type of information that we hold for Church membership is not sensitive and can be distributed to all Church members.

The information that we hold on Children and Youth Clubs membership is a little more sensitive and will be restricted to use by the Children's and Youth Leaders and their Team Members.

The information that we hold on Gym members is more sensitive since it contains health issues information and is therefore treated with even more security. This information will only be available to the operations Manager and the Fitness Instructors.

2. Person Responsible

The person responsible for general security of the building and its operation will also be responsible for Data Protection information security. The Operations Manager is the nominated person.

3. Security Measures

Our current security measures are based on the restricted use of information stored as outlined above. All staff and volunteers are trained and security issues are discussed and imparted during induction procedures. No data processing is done outside of the Centre and only staff and volunteers are used.

4. Physical Security

Our premises are alarmed and all security locks comply with the NACOSS guidelines. The exterior of our building is secured with security fencing, flood lights and security cameras. All information is kept in cloud storage. The Centre is equipped with CCTV, fourteen of which are installed inside the building and two outside. The information is collected and stored on a digital recorder disc and is overwritten every three days. The digital recorder is installed in a locked office. Notices are displayed informing people that CCTV is in operation throughout the premises.

5. Electronic Communication

Definition: Safe use of mobile phones, e-mail, social networking sites etc to communicate with children and young people.

Electronic communication has become enormously important and popular over the past 10 years. It's an easy way to communicate with young people in particular. However, there are dangers that come with it and some choose to use it as a way to meet and groom young people.

Therefore we need appropriate guidelines regarding the safe use of electronic communication, to maintain healthy and safe relationships between adults and children.

It is impossible to cover every area of electronic communication, especially as it changes so rapidly, however, our overriding attitude should be a concern for the people we are working with, and their well being. As long as we are working for their good, then what we do and how we approach our work will dictate our working practices for the good.

The normal boundaries of relationship between youth leader and child must be maintained and electronic communication must never become a substitute for face to face contact with young people.

General

Parents/carers and children/young people have the right to decide if a worker is to have email addresses or mobile phone numbers, and shouldn't be pressurised into giving that information.

If electronic communication is going to be used then BCLC's safeguarding policy should acknowledge it as a legitimate means of communicating with children and young people, and include an expectation regarding their use.

Any one using electronic communication to contact children or young people on behalf of BCLC should be vetted in the same way as people who work face to face with young people.

Communication between children and adults by whatever method should take place within clear and explicit boundaries. Adults should not share any personal info with children or young people, and should not request or respond to any personal information from the child other than that which is necessary and appropriate as part of their role. Adults should ensure that all communications are transparent and open to scrutiny.

Adults should be careful in their communications with children or young people so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. To reduce risk of misinterpretation use clear unambiguous language and avoid the use of unnecessary abbreviations and ambiguous text language.

With all electronic communication there should be a reasonable cut off time, such as 10pm – 7am. Cases of emergency maybe exception to this rule but must be reported and recorded.

It is the youth leader's responsibility to set the boundaries on electronic communication, they should not be communicating with young people in this way at all hours of day and night.

Contact with young people by electronic communication should be for information giving purposes only, not just general chatter.

Consent

If electronic communication is to be used to contact children or young people, written consent should be obtained from the parent/carer. Direct communication with children of primary school age and below is not advised.

Internet Access

BCLC provides internet access for children/young people. Parent/carers and children/young people should sign a user agreement, which explains what is acceptable/ unacceptable online. Adequate parental control filters should be in place, and children and young people should be supervised by an adult whilst using the computers.

E-mail

E-mails should be sent out with BCLC youth header and footer showing the young person this is an official communication from a member of the youth team.

Chat and Instant Messenger

Use of instant messenger services should be kept to a minimum.

However, recognising that a young person in need/crisis may use this as a way of communicating; significant conversations should be saved as a text file if possible, and a log kept of who and when they communicated.

Mobile phones

It is unreasonable to expect BCLC to provide mobile phones for volunteers, so safeguards need to be built in here.

Mobile phone usage should be primarily about information giving. 'Text language' should be avoided so that there is no misunderstanding of what is being communicated. 'Text Conversations' should usually be avoided; not finishing off with a kiss or any other words that could be misunderstood (that is a series of text messages/emails being sent to and from youth leader and young person)

Cameras on mobile phones

The use of the camera should comply with BCLC's policy on photo's/videos.

It would be unwise to keep images of a children or young people on workers mobile phones.

Social Networking Sites

If youth leaders are going to communicate via social networking sites they should ensure their site is appropriate for young people to see. Lower age limits of social networking sites should be adhered to (this varies from site to site). Be aware of the content of photos that may be uploaded on to your site.

All communication with young people should be kept within public domains.

Separate sites should be used for personal use and for youth leader use, e.g.

Ian Naftel would have a personal site for friends, family and so on and if he wants to communicate with young people from BCLC youth work, Ian should have an 'Ian Naftel – Youth Leader' site, where communication with young people takes place. This is easier to do on some sites than others, the alternative to this would be to have a youth group site where all information remains in the public domain.

Young people should not be accepted as 'friends' on youth leader's personal sites.

For further information

Take a look at CEOPs website - [Child Exploitation and Online Protection](http://www.ceop.gov.uk)

Updated 20/9/2016
Operations Manager