# The Parish of Broughton St John Baptist

# e-Safety & Acceptable Use Policy

To be read alongside the Parish Safeguarding Policy 2018

Reviewed & adopted by the Parochial Church Council at a meeting on 14th May 2018.

Signed on behalf of the PCC by: Shaun Baldwin

Rev'd Shaun Baldwin, Vicar & Chairman of PCC

**1. e-safety Definition**

e-Safety – or electronic safety is the collective term for safeguarding involving the use of mobile (cell) phones, computers (laptops, netbooks, tablets) and other electronic devices including games consoles, to communicate and access the Internet, emails, texts messages (SMS), Instant Messaging (IM), social networking sites (SNS) and other social media; often referred to as Information and Communications Technology (ICT).

The technology is constantly advancing bringing with it additional safeguarding considerations. An e-safety policy should be adopted and adapted to reflect all communications between workers and children/young people (those under 18 years of age) recognising the merging between online and offline worlds and the distinctiveness and difficulties within faith based organisations of defining clear boundaries for everyone.

The e-safety policy should include guidance on both fixed and mobile internet technologies. e.g. PCs, laptops, tablets, web cams, digital video equipment, mobile phones, personal digital assistants (PDAs), digital cameras and portable media players or any other forms of mobile communication device being used.

**2. The organisation/centre commitment to e-safety**

We will exercise our right to monitor the use of our computer systems. This will include access to websites, the interception of e-mail and the deletion of inappropriate material where it believes unauthorised use of the computer system is or may be taking place, or the system is or may be being used for a criminal purpose or for storing unauthorised or unlawful text, images or sound.

When using a computer or electronic device with Internet at the centre, children will not be permitted to:

- Search for and/or enter pornographic, racist or hate-motivated websites;
- Download, forward-on, copy or burn onto CD any music, images or movies from the internet where permission has not been granted by the copyright holders;
- Disclose any personal information e.g. addresses (postal, email or messenger), telephone numbers, bank details. This includes personal information about another person;
- Send or display offensive messages or pictures;
- Use obscene language;
- Violate copyright laws;
- Trespass in others' folders, work or files (i.e. enter without permission);
- Retrieve, send, copy or display offensive messages or pictures;
- Harass, insult, bully or attack others;
- Damage computers, computer systems or computer networks;
- Use another user's password; or
- Use computers for unapproved commercial purposes.

**Sanctions:**

- Violations of the above rules will result in a temporary or permanent ban on Internet use.
- Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.
- When applicable, police or local authorities may be informed.

**3. Children and Young People will be expected to make appropriate and safe use of ICT**

Children and young people will be required to agree to the following expectations for responsible Internet use:

- Where using a network or similar I will use only use my own login and password which will be kept secret
- I understand that I must not bring software into the church/organisation without permission
- I am responsible for e-mail that I send and for contacts made. I will only send messages which are polite, sensible and free from unsuitable language.
- I will ensure that they are carefully written. I will not send any attachments which are hurtful, abusive or offensive.
- If I receive anything, see anything or come across a website which may be unsuitable or makes me feel uncomfortable I will immediately tell a responsible person [name/title of worker].

- I understand that I must never give my home address, phone number, send photos, give out personal information, or arrange to meet someone who contacts me over the internet.
- I will not send anonymous messages and I know that chain letters are not permitted.
- I understand that if I deliberately break these rules, I will not be allowed to use the Internet and/or e-mail and that my parents/carers will be informed.

**Rationale:**

When a child or young person joins a group, club or activity, responsible ICT use should be included on the general consent form the parent/carer signs (i.e. that ICTs are operating and may be used to communicate with their child).

The centre's e-safety policy should be attached to the consent form.

It is the joint responsibility of workers, the centre and the parent or guardian of the child to educate them about their responsibility when using the Internet.

If the parent/carer requests their child is not communicated with via ICTs, this must be respected and an alternative found.

This responsible Internet Use statement helps to protect children by clearly stating what use of the computer resources is acceptable and what is not.

This agreement should be signed by the child, their parent/carer and the church/organisation.

**4. We will make appropriate Use of any Photographic and/or Video Images taken during centre activities**

Clear guidelines must be operated when taking photographic and video images of young people involved in centre activities as follows:

- Photographs that include children will be selected carefully and will not enable individual children to be clearly identified.
- Children's full names will not be used anywhere on the web site in association with photographs.
- Permission will be sought before any images are taken and/or displayed. Images should only be used for the specific purpose agreed by the person photographed.
- Written consent must specify what purposes the image will be used for, and how it will be stored if not destroyed.
- If the intention is to use an image on the internet, this must be clearly stated at the time that consent is sought.
- Further written consent is required if images are to be used in other ways than originally specified.
- When using photographs of children, use group pictures and never identify them by name or other personal details. These details include e-mail or postal addresses, telephone or fax numbers.
- Ensure that any use of images reflects the diversity of age, ethnicity and gender of the activity.

**Rationale:**

Parents will be given the opportunity to decide if they want pictures of their son/daughter to appear on the website. A list of parents who do not require their son/daughter to appear on the website should be kept and regularly updated.

This ensures that privacy is respected and no embarrassment is caused.

The policy should apply to all images and audio content be it still photographs, films or audio clips. Images count as personal data under the Data Protection Act 1998.

Newspapers and other print media are bound by the Press Complaints Commission Code of Practice. Legitimate journalism is a 'special purpose' under the Data Protection Act, which exempts it from the requirement of security, but there are numerous restrictions on photographing children.

**5. We will ensure that appropriate safeguards are in place, including the use of filtering software on all computers used within the centre**

To ensure that unwanted and unsolicited information, viruses and other malware does not intrude on the use of ICT, centres will ensure all appropriate and reasonable steps are taken to protect computers and the users of them as follows:

- Filtering software will be installed on all computers used at the centre or as part of any activities operated by the centre.
- On centre websites, details are prominently displayed as to where to find help online including having the CEOP button on the web site.

**Rationale:**

To ensure the integrity of the system and to protect children ensure that filtering software, firewalls etc are enabled.

**6. We will respond appropriately and sensitively to all e-safety concerns.**

Where concerned that there may be an e-safety incident, this will be reported to the centre's designated safeguarding officer in the same manner as the reporting of any other safeguarding concern. They can then determine if the matter should be reported to the statutory authorities or other appropriate agencies e.g. CEOP.

**Rationale:**

Follow the e-safety flow chart for assistance with this.

**7. We will operate safe email communications with children and young people.**

When using email to communicate with children and young people, workers should:

- Obtain parental agreement before they use email services to communicate with a child or young person; and
- Use clear, unambiguous language to reduce the risk of misinterpretation (e.g. workers should never use terms such as 'luv' to round things off).

**Rationale:**

Ensure all messages can be viewed if necessary by the worker's supervisor and this policy is explained to children and young people. Although unlikely to happen, this can help deter bullying, insulting or abusive emails

**8. We will make use of appropriate confidentiality clauses in all email correspondence.**

All email should contain an appropriate clause regarding confidentiality as follows:

*Any views or opinions presented are solely those of the author and do not necessarily represent those of the Parish of Broughton St John Baptist unless otherwise stated. If there is a concern, e.g. that the sender or someone else, particularly a child, may be at risk of serious harm, we may need to share those concerns. In such circumstances we will inform the sender giving details of who would be contacted and what information would be given.*

**Rationale:**

Children can find it easier to communicate via email as nobody is physically present. This means the child may be more willing to share personal and sensitive information about themselves or a given situation than they would face to face.

Whilst it is entirely appropriate to offer general advice and support, counselling should only be done by those qualified to give it. In any event it is advisable to add a rider to the bottom of any email stating the level of confidentiality.

**9. We will make appropriate use of mobile phones where they are needed.**

Mobile phones should only be used where necessary and will be guided by the following considerations:

- Where appropriate use group rather than individual texting.
- Take care with the language they use, avoiding ambiguous abbreviations such as 'lol' which could mean 'laugh out loud' or 'lots of love' and always end with their name.
- Any texts or conversations that raise concerns should be saved and passed on/shown to the worker's supervisor.
- Any images of children taken on a mobile phone should be downloaded to the church / organisations' computer and kept securely.
- Workers should not keep images of children on their mobile phone.
- Workers should not as a general rule give out their personal mobile number to children. The centre recognises that this may be needed at times (with the agreement of the parents and leaders).
- As well as ensuring that calls / texts are not sent after 9pm also ensure that calls and texts are not sent whilst the child is at school / college (9am-4pm), as this may be against the educational establishments rules.
- Workers should enable a password/lock on their phone for data protection and do not allow unauthorised access.
- Workers should not make contact with young people after 9pm at night.

**Rationale:**

Not every child or young person has the use of a mobile phone and, even if they do, parents may not want the worker to have the number. It is important therefore to have alternative means of communication.

It is advisable that a worker be supplied with a work-dedicated phone. This way all calls and texts can be accounted for via an itemised phone bill. It also protects the worker's right to a personal life outside work. Equally workers should make it clear that a work phone is what it says it is and not divulge their personal mobile number to the children/young people they work with.

Many mobile phones have digital cameras. Workers should ensure that they only take photographs of children and young people in accordance with the e-safety policy on photography (e.g. ensure that consent is obtained and all images are stored in accordance with Data Protection Act principles).

Recognise that text messaging is rarely an appropriate response to a young person in a crisis situation or at risk of harm .

**10. We will consider the appropriate use of Chat & Messenger Services and whether these are necessary.**

Workers should ensure that all communications using IM services adhere to the following:

- Communication will not take place between the hours of 9 pm and 9 am
- Workers should ensure that they enable settings when using IM services which allows for conversations to be saved as text files.
- Children/young people should be made aware that conversations will be recorded and kept (via text files or similar).

**Rationale:**

Instant Messenger Services or IM (e.g. MSN Messenger, AOL, AIM) are internet programs that allow people to write and receive messages in real time. Many young people use IM for both one-to-one (chat) and group conversations (chat rooms). Chat is a great way to engage with young people but workers should consider the following:

There should be an agreed length of time for a conversation and a curfew e.g. no communication between 9 pm and 9 am.

To ensure accountability and safeguard integrity, workers should save significant conversation as a text file as well as keep a log of when and with whom they communicated. This should be explained to children and young people.

The same protocols for workers communicating with children and young people via email and mobile phone should apply to IM. In other words, care needs to be taken with regard to language and content as well as when and for how long a communication lasts.

Enhanced IM services using technology such as web cams or Skype (voice calls over the internet) also require procedures for use by workers.

**11. We will make safe and appropriate use of social networking sites when communicating with young people.**

When using social networking sites (e.g. Facebook, MySpace, Bebo etc..), we will ensure that the following guidance is used by all workers:

- Workers should not add young people to their personal social networking page if they are involved with the youth activities and are under the age of 18.
- Workers should in preference set up a Facebook group / Fan page for the centre and invite young people to be members. (If they are over the required minimum age limit i.e.: 13 for Facebook).
- Workers should only use an agreed social networking account for contact with young people with whom they are working. This should normally be an account set up specifically for this purpose on behalf of the centre rather than an individual.
- Workers should seek to ensure that their personal profiles on any social networking sites should be set to the highest form of security to avoid young people accessing personal information or seeing any pictures of a personal nature.
- Messages sent to young people regarding youth activities should be posted openly and 'inbox' messaging should be avoided. If this is necessary in exceptional circumstances, a copy should be sent to the manager of the activity/centre to assist transparency.

**Rationale:**

Use of social networking sites by workers makes it harder to boundary their private life, and also opens up the possibility of relationship between 'friends' who are children and 'friends' who are from the workers' adult personal world

There are risks both for children and also for workers, who may find images and text appearing on their profiles which can be damaging to their reputations and positions as role models.