



**E-safety Policy**

to be read in conjunction with

St Mark’s Child Protection Policy

and Vulnerable Adults Policy

**Policy and Procedures**

**The Parish**

**of**

**Bestwood St Mark**

**Background**

The use of information and communication technologies (ICT), including the Internet, has developed rapidly and now involves many members of all ages at St Mark’s. The internet has become an integral part of peoples’ lives, providing access to information and networking for social, business and educational purposes. Churches are more and more regularly using “new media” to communicate not just with their members but also the world in which they exist. By linking this Policy with our Child Protection Policy and Adults at Risk Policy we seek to promote the safe use of new technology and media by all members of our church community.

1. **Introduction**
   1. The internet offers great opportunities for the Church both in the way we communicate with the wider world and how we discuss matters amongst ourselves. It is faster, cheaper and more widely available than “old media” but does not change our understanding of confidentiality, responsibility or Christian witness.
   2. The nature of the internet means the distinction between public and private conversations can be blurred. However, conversations, emails, reports and minutes to church leadership, PCC or other bodies remain confidential unless explicitly released from their confidential status.
2. **E-Safety**

At St Mark’s we recognise the range of e-safety issues and plan accordingly to help ensure the appropriate, effective and safe us of electronic communication within our church.

Our E-Safety Co-ordinator is:

**Kirsty Cowley**

Tel: 07906045084 Email: kirsty.cowley@ntlworld.com

E-Safety encompasses not only internet technologies but also electronic communication such as mobile phones and wireless technology. It highlights the need to ensure all our church members are aware of the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences. The internet is an unmanaged, open communications channel.

**Why use the internet in the life of St Mark’s?**

* St Mark’s Facebook page and website are a means of sharing information and resources across the church community and making relevant information about St Mark’s available to those who wish to find out about us.
* Internet use and text messaging are key methods of communicating with teenagers and/or their families.
* Use of the internet enables fast, efficient environmentally friendly sharing of information documents and media.

1. **Access**

The internet is widely available across a range of devices. As a result, we are unable to control everything a web user might see while on church premises or at a church event. At St Mark’s we take the following precautions to minimise this risk and ensure that users access only appropriate information:-

* 1. Internet access is not readily available at St Mark’s. If or when it is available on the church laptop then under 18’s should have only supervised access.
  2. As ease of access and the number of access points increase we will review the need for filtering software.
  3. Group leaders should always preview websites they anticipate using with groups, including any material on them and assess their suitability for their group.
  4. Church members are encouraged to inform a member of the Clergy, the E-Safety Co-ordinator and/or Churchwardens immediately they encounter any material that upsets them, they feel is offensive or they feel may cause offence to others. This could include, but is not limited to, offensive language, racist, sexist or sexualized material.

3.5 The E-Safety Co-ordinator, a member of the Clergy or Churchwardens deal with any incidents involving misuse of the internet. The incident is recorded in the E-safety log (see Appendix 1).

3.6 All leaders must accept the terms of the policy before using any internet resource at Church.

3.7 When copying materials from the web, copyright laws must be respected.

**4. Using e-mail, text message and other forms of direct messaging**

All direct messaging should be used responsibly and the following precautions followed at all times:

4.1. Contact details should be treated as confidential and should not be passed on without consent.

4.2. When contacting those under the age of 18:

* The message should be sent from a church or public address or number if possible, although it is accepted that this is not always possible.
  + Messages and their responses should not be deleted unless a copy has been made
  + Messages should be sent to more than one recipient including one of the following an incumbent or other member of clergy, churchwarden or E-safety Co-ordinator

1. **Social Media and Church Website**

St Mark’s has developed a website and a presence on social media. These contain information about the ethos and values of the church, the staff structure, details of past and future events and other relevant information. The sites, pages and feed are updated and their content reviewed on a regular basis to ensure that it is well presented and that personal security is not compromised. The church takes the following precautions to ensure the security of its members and visitors is maintained:

5.1 The PCC delegates authority to administer the church’s on-line presence to the Website and Social Media Administrator and the PCC and other church leaders agree to provide him/her with up to date information for inclusion on-line. St Mark’s Social Media and Website Administrator is Mrs Kirsty Cowley. All content published is monitored by the incumbent and/or churchwardens.

5.2 Names of individual members of staff and church leaders may be included on-line but with personal information will be limited.

5.3 Named photographs of children and young people are not published. Any group photographs do not have a name list attached.

5.4 Wherever possible photographs with smaller images of children are used to minimise identification of individual children.

5.5 Checks are made that all people in photographs are appropriately clothed.

5.6 Parental permission is obtained for all children and teenagers whose photographs appear on the Facebook page and website. If practicable the consent of teenagers should be obtained prior to using their photographs. It is good practice to have written consent to use photographs although verbal consent will suffice.

1. **Personal Publishing**

St Mark’s acknowledges the increasing value of social networking and personal publishing but encourages all members to act responsibly to ensure safety. All congregation members are encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo or address once published. In particular when:

6.1 Posting photos and videos on any social network space.

6.2 Sharing personal information such as addresses, date of birth etc.

6.3 Being identifiable through the use of names, photographs and avatars.

**7. Group Activities and Church Leadership**

St Mark’s wishes to encourage good practice amongst the leadership: that is clergy, Readers, leaders of all groups, pastoral care team and PCC members

7.1 Mobile phones provide access to many forms of new media and should only be used appropriately. Group leaders have the right to restrict or prohibit the use of mobiles at their discretion during group activities.

7.2 No adult leaders should be in one to one communication with children and young people outside of recognised church activity times.

* 1. Adult leaders should not have young people as their ”friends” on Facebook etc. or publish images of children and young people in their personal pages (unless permission is given by the children’s parents.)
  2. No leader should take or publish personal details of children and young people. No names, home or email addresses, school or mobile numbers.
  3. Leaders must be careful how they use photos of children: if a child is named, then avoid using their image; if an image is used, avoid naming the child, obtain children’s and parents’ consent to use photographs on websites.
  4. Leaders should think before they post. Always seeking the permission of the children, young people and their parents before adding them to your social network page.

Young people are advised to talk to a responsible adult if they suspect a site or their details are being used inappropriately.

**8. Emerging Internet Applications**

Many emerging communication technologies offer the potential to develop new teaching and learning tools. Mobile communications, wide internet access and multimedia present opportunities which need to be evaluated to assess risks, to establish benefits and to develop good practice. As new technology emerges we will review and update this policy as necessary.

**9. ICT System Security**

We will ensure that the church laptop is protected with anti-virus software and firewalls.

We ask that all employed staff and all office holders (eg: wardens, treasurer, secretary) of St Mark’s to protect their own laptops and PC’s with anti-virus software and firewalls.

**10. Data protection**

St Mark’s complies with all requirements under the Data Protection Act 1998 with regard to storage of information concerning individuals.

10.1 The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual).

The eight principles are that personal data must be:

* Processed fairly and lawfully
* Processed for specific purposes
* Adequate, relevant and not excessive
* Accurate and up to date
* Held no long than is necessary
* Processed in line with individuals’ rights
* Kept secure
* Transferred only to other countries with suitable security measures

10.2 All personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998.

10.3 Personal data may only be disclosed without consent where there is a clear child protection concern and only to the appropriate services and authorities.

**11. E-Safety Co-ordinator**

The key responsibilities of the E-Safety Co-ordinator include:

* Developing an e-safe culture and acting as a named point of contact on all e-safety issues, promoting the St Mark’s e-safety vision to all stakeholders.
* Maintaining an e-safety log.
* Monitoring and reporting on e-safety issues to the Safeguarding Co-ordinator, Clergy, Pastoral Care team and PCC and other agencies. A decision will then be taken as to whether any referrals need to be made.
* Reviewing and updating e-safety polices.

The procedures and guidelines were last reviewed and agreed by the Parochial

Church Council in 2017

Date:

Signed by the Churchwardens:

…………………………………………………

…………………………………………………

**Date for policy review**

The Parochial Church Council will review this E-Safety Policy and how it is to be

implemented by 2018

Appendix 1: E-Safety Log

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Concern Notified by | Details of Concern | Concern Resolved/ Passed on |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |