



E-Safety Policy

**The Parochial Church Council of the Ecclesiastical Parish of
All Saints, Patcham**

Policy adopted by PCC 21 November 2022

This policy will be reviewed by the PCC at least annually and will be amended if necessary to take account of any Diocesan Policy changes. It will not be reissued unless it is amended, so this version will remain in force until withdrawn.

Parish E-Safety Policy

This policy should be read alongside the Parish of All Saints Patcham's policies on Safeguarding, Whistleblowing, and Raising Safeguarding Concerns.

This policy applies to all staff, including clergy, PCC members, paid staff, volunteers including children's and youth workers, those involving in leading or coordinating music and worship, and anyone else involved in working or volunteering on behalf of All Saints, Ascension or the parish.

Purpose of Policy

To protect children and young people who are ministered to by All Saints & Ascension and who make use of information technology (such as mobile phones/devices, games consoles and the Internet) as part of their involvement with the parish.

To provide our staff, volunteers, and parents with the overarching principles that guide our approach to e-safety.

To ensure that, as a Christian community, we minister in line with our values, and also within the law, in terms of how we use information technology and behave online.

To guide us as we seek to equip the children and young people with whom we minister to be safe, discerning and wise users of information and communication technology.

We recognise that:

The welfare of the children and young people to whom we minister and with whom we come into contact is paramount, and should govern our approach to the use and management of electronic communications technologies and online behaviour;

All children, regardless of age, disability, gender, racial heritage, religious belief, sexual orientation or identity, have the right to equal protection from all types of harm or abuse;

Working in partnership with children, young people, their parents, careers and other agencies is essential in promoting young people's welfare, and in helping young people to be responsible in their approach to e-safety;

The use of information technology is an essential part of all our lives; it is involved in how we as a church gather and store information, as well as how we communicate with each other. It is an intrinsic part of the experience of children and young people, and is greatly beneficial to all. However, it can present challenges in terms of how we use it responsibly, and, if misused either by an adult or a young person, can be actually or potentially harmful.

We will seek to keep children and young people safe by:

Treating any child protection concern arising from the online world in the same way, taking it just as seriously, as concerns arising from the offline world.

Ensuring that our parish safeguarding officer has access to up-to-date information and training regarding online safety, assisting them as appropriate to access this training.

Ensuring that all staff and volunteers at All Saints & Ascension avoid using private forms of electronic communication (text message, email, direct messaging including on social media) to communicate with the children and young people they are responsible for.

Taking the use of such private communication between staff or volunteers and young people as seriously as one-on-one contact between adults and children without another responsible adult present. It is always the responsibility of the adult staff member or volunteer to put appropriate boundaries in place in their relationships with the young people with whom they minister, in both the offline and online worlds.

Using open online forums to communicate with children, such as Facebook youth group pages to notify young people of events etc.

Avoiding any form of inappropriate content in what we, our staff and our volunteers post online, including (but not limited to) sexual content, racist, sexist or otherwise bigoted content, or content promoting illegal activity.

Maintaining electronic versions of sensitive personal data securely, according to the principles of the Data Protection Act.