

Benefice of Malpas, Threapwood and Bickerton

Guest Wi-Fi, Online Safety and Acceptable Use Policy

Policy status

This policy supplements the following parish policies and procedures:

- Parish Safeguarding Policy;
- Data Protection Policy and Privacy Notice;
- Policies and procedures governing work with children, young people and vulnerable adults;
- Church of England safeguarding guidance and codes of practice.

It applies to:

- St Oswald's Church, Malpas;
- St John's Church, Threapwood;
- Holy Trinity Church, Bickerton;
- any church hall, meeting place or activity for which one of the PCCs provides internet access.

This policy should be adopted separately by each PCC.

1. Purpose

The churches provide guest Wi-Fi as a service to worshippers, visitors, volunteers, community groups and those attending church activities.

The purpose of this policy is to ensure that church internet access is:

- safe and appropriate;
- consistent with the Church's safeguarding responsibilities;
- separated from confidential church administration;
- used lawfully and respectfully;
- managed in accordance with data-protection requirements.

Access to church Wi-Fi is a privilege and may be restricted, suspended or withdrawn where necessary.

2. Our principles

When providing internet access, the PCC will seek to:

1. promote the safety and wellbeing of children, young people and vulnerable adults;
2. provide appropriate filtering and security;
3. respect users' privacy;
4. collect and retain no more personal information than is necessary;
5. respond appropriately to safeguarding, security or criminal concerns;
6. encourage behaviour online that is safe, kind, lawful and respectful.

Filtering is an important safeguard, but no filtering system can guarantee that all unsuitable content will be blocked.

3. Church networks

The church will maintain two separate networks:

Private church network

The private network is reserved for authorised church officers, church-owned equipment and approved operational purposes.

It may be used for:

- church administration;
- financial and giving systems;
- parish records;
- safeguarding administration;
- printers and other church equipment;
- livestreaming and worship technology;
- other authorised church business.

The private network password must not be displayed publicly or given to visitors, hirers or congregation members.

Guest network

Visitors and people attending church activities should be directed to the guest network.

The guest network will, so far as the available service permits:

- be separated from the church's private network;
- have content filtering and security controls enabled;

- prevent users from changing network settings;
- be reviewed periodically to ensure that the filtering remains active and appropriate;

Church-owned devices containing personal, financial, confidential or safeguarding information should not normally use the guest network.

4. Acceptable use

Church guest Wi-Fi may only be used for lawful, safe and appropriate purposes.

Users must not use the network to:

- access, create, download, store or distribute illegal material;
- access or share sexually explicit, abusive, violent or otherwise seriously inappropriate material;
- bully, harass, threaten, exploit or humiliate another person;
- engage in grooming, coercion or abusive communication;
- promote hatred, terrorism, extremism or violence;
- breach another person's privacy or share personal information without authority;
- share photographs or recordings of other people without appropriate permission;
- infringe copyright or other intellectual-property rights;
- gain unauthorised access to another device, account, network or service;
- introduce viruses, malware or other harmful software;
- interfere with the operation of the network;
- attempt to bypass content filters, security controls or access restrictions;
- use the network for fraudulent, criminal or seriously disruptive purposes.

Reasonable personal use is permitted. The PCC may restrict excessive use where it affects the availability or performance of the service for others.

5. Children and young people

Children and young people are welcome to use the guest Wi-Fi, subject to this policy and any rules established for the particular activity.

During organised church activities:

- leaders may limit or prohibit the use of personal devices;
- children and young people should be given clear, age-appropriate guidance about safe internet use;

- leaders should provide supervision appropriate to the children's ages and the nature of the activity;
- children and young people should be encouraged to tell a trusted adult if they encounter anything online that worries, frightens or upsets them;
- children should not be asked to investigate, save or show harmful material to other children;
- filtering must not be treated as a substitute for appropriate leadership and supervision.

A child-friendly Wi-Fi statement will be displayed or made available where children and young people regularly meet.

Provision of Wi-Fi does not authorise church officers or volunteers to communicate privately with children or young people. All electronic communication must comply with the parish safeguarding and communications policies and current Church of England guidance.

Church officers must not use private or disappearing-message channels to avoid appropriate accountability or safeguarding oversight.

6. Communications, photographs and social media

The availability of church Wi-Fi does not change the rules governing photographs, videos, livestreaming, social media or electronic communication.

Church officers and volunteers must:

- use approved church accounts or communication channels where these are available;
- maintain appropriate boundaries;
- avoid secretive or inappropriate private communication;
- obtain appropriate permission before publishing identifiable photographs, videos or personal information;
- avoid identifying or disclosing confidential or safeguarding information;
- report concerning online behaviour in accordance with the Parish Safeguarding Policy.

No person should assume that permission to attend a church activity is also permission for their image, personal information or online activity to be published.

7. Safeguarding concerns

Any safeguarding concern arising from internet or Wi-Fi use must be taken seriously.

This may include:

- online grooming or exploitation;
- cyberbullying;
- threats, harassment or coercion;
- sexualised communication involving a child;
- sharing intimate or abusive images;
- evidence that a child or vulnerable adult may be at risk;
- access to material that may indicate abuse or criminal activity.

A person receiving a concern should:

1. respond calmly and take what they are told seriously;
2. avoid promising complete confidentiality;
3. make a factual written record;
4. report the matter without delay to the Parish Safeguarding Officer;
5. follow the parish and diocesan safeguarding reporting procedure.

The person receiving the concern must not conduct their own investigation, search through someone's device or ask others to view harmful material.

Suspected illegal images or content must not be downloaded, copied, printed, forwarded or circulated. Advice should be sought promptly from the Parish Safeguarding Officer, Diocesan Safeguarding Team or police.

Where a child or another person is at immediate risk of harm, the emergency services must be contacted by calling **999**.

Parish Safeguarding Officer

Name: _____

Telephone/email: _____

Diocesan Safeguarding Team

Contact details: _____

8. Data protection and privacy

The PCC will manage any personal information connected with Wi-Fi provision in accordance with the UK GDPR, the Data Protection Act 2018 as amended, its Data Protection Policy and its Privacy Notice.

Depending on the equipment and internet provider, technical information may be generated when a device connects to the network. This may include:

- the device or network address;
- the date and time of connection;
- the IP address allocated to the device;
- security or filtering alerts;
- limited network-traffic information.

The PCC will:

- not require names or contact details merely to access guest Wi-Fi unless there is a clear reason for doing so;
- not routinely monitor the content of people's personal communications;
- access technical records only where necessary for security, troubleshooting, safeguarding or the investigation of suspected misuse;
- restrict access to any records to authorised people;
- retain information only for as long as it is needed;
- store any downloaded records securely;
- not use connection information for advertising or unrelated purposes;
- provide appropriate privacy information where the PCC itself collects or accesses identifiable connection data.

The internet provider or equipment provider may process technical information under its own terms and privacy arrangements.

Information may be shared with the Diocesan Safeguarding Team, police, statutory authorities or professional advisers where this is lawful, necessary and proportionate.

9. Network administration and security

The PCC will appoint a limited number of authorised people to administer the network.

Network administrators must:

- use strong and unique administrative passwords;
- keep administrative login details confidential;

- change passwords when an authorised administrator leaves their role or where a password may have been compromised;
- apply security updates where these are under the church's control;
- check periodically that guest-network separation and filtering remain active;
- avoid making unnecessary copies of connection records;
- report suspected security or data breaches promptly;
- not use administrative access to view information out of curiosity or for an improper purpose.

The names of authorised administrators will be recorded by the PCC or Standing Committee.

Authorised administrators

10. Misuse and incidents

Where misuse is suspected, the church may:

- ask the person to stop;
- disconnect or block a device where technically possible;
- change the guest password;
- temporarily suspend the guest network;
- preserve limited technical information relevant to the incident;
- contact the internet provider;
- report safeguarding concerns under church procedures;
- report suspected criminal activity to the police;
- consider whether a personal-data breach has occurred.

Any personal-data or network-security incident must be reported promptly to the incumbent, churchwardens and the person responsible for data protection if this is a different person.

A proportionate record should be kept of the incident, the advice received, the decisions made and the action taken.

11. Hirers and outside groups

Guest Wi-Fi may be offered to organisations hiring or using church premises.

Hirers and group leaders:

- must comply with this policy;
- remain responsible for the conduct and supervision of their participants;
- must take appropriate steps to supervise children and vulnerable adults;
- must report safeguarding or security concerns to the church contact;
- must not be given access to the church's private administrative network.

The church does not guarantee that Wi-Fi will always be available, uninterrupted or suitable for a hirer's particular purpose.

Serious or repeated misuse may result in Wi-Fi access being withdrawn and may affect future use of the premises.

12. Responsibilities

The PCC

The PCC is responsible for:

- adopting and reviewing this policy;
- ensuring reasonable network security and filtering;
- appointing authorised administrators;
- ensuring appropriate safeguarding and data-protection arrangements.

The incumbent and churchwardens

The incumbent and churchwardens provide oversight of the policy and respond to serious operational or security concerns.

The Parish Safeguarding Officer

The Parish Safeguarding Officer advises on and receives safeguarding concerns arising from online activity.

Network administrators

Network administrators maintain the technical settings and report concerns or incidents.

Group leaders and hirers

Group leaders and hirers are responsible for explaining appropriate use and supervising participants where necessary.

Individual users

Each user is responsible for their own lawful and appropriate use of the network.

13. Availability of the policy

A brief acceptable-use statement will be displayed alongside the guest Wi-Fi details.

The complete policy will be available:

- on request;
- from the incumbent, churchwardens or Parish Safeguarding Officer;
- on the parish or benefice website where appropriate.

14. Review

This policy will be reviewed:

- annually;
- following a significant safeguarding, security or data-protection incident;
- when the internet provider or network arrangements change;
- when relevant Church of England guidance or legislation changes.

Approval

PCC of St Oswald's Malpas and St John's Threapwood

Adopted on: _____

Minute reference: _____

Signed on behalf of the PCC: _____

Next review due: _____

PCC of Holy Trinity Bickerton

Adopted on: _____

Minute reference: _____

Signed on behalf of the PCC: _____

Next review due: _____

Notices to be displayed in churches by the Wi-Fi password.

Appendix 1: Guest Wi-Fi Notice

Using Our Church Guest Wi-Fi

Guest Wi-Fi is provided for lawful and appropriate use by visitors and those attending church activities.

The guest network is separate from the church's private administrative network and is subject to content filtering.

Please do not use the Wi-Fi to:

- access or share illegal, offensive, abusive or harmful material;
- bully, threaten or harass anyone;
- interfere with the network;
- attempt to bypass its filters or security settings;
- place another person's privacy or safety at risk.

Filtering cannot guarantee that all unsuitable material will be blocked.

Access may be restricted or withdrawn where the network is misused. Safeguarding or criminal concerns may be reported to the appropriate authorities.

By using the guest network, you agree to use it safely, lawfully and respectfully.

Appendix 2: Children and Young People's Wi-Fi Notice

Using Our Church Guest Wi-Fi

You are welcome to use the church guest Wi-Fi.

Please use it in a way that is safe, kind and respectful.

- Only look at and share things that are appropriate.
- Do not use the Wi-Fi to bully, threaten or upset anyone.
- Keep your passwords and personal information private.
- Do not share photographs or videos of other people without permission.
- Do not try to change the Wi-Fi settings or get around its safety filters.
- If you see something that worries, frightens or upsets you, close it and tell a trusted adult straight away.

The Wi-Fi has safety filters, but they may not block everything.

Using the Wi-Fi means you agree to these rules. If the Wi-Fi is misused, access may be removed.

Be safe. Be kind. Ask for help.