



## A Blessing to Cuckfield

The Parochial Church Council of Holy Trinity Cuckfield  
UK Registered Charity No. 1131432

### **Holy Trinity Church Cuckfield PCC Data Protection, Privacy & Information Governance Policy**

*This policy is designed to ensure compliance with the UK General Data Protection Regulation (UK GDPR); the Data Protection Act 2018; the Privacy and Electronic Communications Regulations (PECR); the Data (Use and Access) Act 2025; safeguarding obligations; applicable Church of England guidance; charity law obligations; and relevant aspects of the Online Safety Act 2025.*

**Adopted by:** The Parochial Church Council (PCC) of Holy Trinity Church Cuckfield  
**Version:** June 2026  
**Review date:** Annual review, earlier if legislation, Diocesan, ICO, or Charity Commission guidance changes  
**Policy owner:** PCC/PCC Secretary (Data Protection Lead)

#### **1. Purpose of this Policy**

This policy sets out how Holy Trinity Church Cuckfield ('the Church', 'the PCC', 'we', 'us' or 'our') collects, uses, stores, shares and protects personal information in a compliant fashion.

The policy applies to PCC members; clergy; employees; volunteers; ministry teams, and any group or committee operating under the PCC's charity number; church officers; contractors; pastoral visitors; safeguarding officers; livestream and media teams; and anyone processing personal data on behalf of the PCC.

This policy should be read alongside other PCC policy guidelines such as the Church safeguarding policy; complaints procedure; social media and WhatsApp policy; CCTV policy; records retention schedule; staff and volunteer codes of conduct; bullying and harassment policy; and IT and cybersecurity procedures.

#### **2. Data Controller**

The data controller is:

The Parochial Church Council of Holy Trinity Church Cuckfield  
The Church Office  
The Old School  
Church Street  
Cuckfield  
West Sussex RH17 5JZ

Email: [office@holytrinitycuckfield.org](mailto:office@holytrinitycuckfield.org)  
Telephone: 01444-456461

The PCC is a charity and forms part of the Church of England. In addition to the incumbent and clergy team, the PCC may also where appropriate work jointly with some or any of the following: the Diocese of Chichester; the Bishop of Chichester and diocesan bodies; Church of England safeguarding bodies; and other churches or church charities undertaking joint ministry activities. Where data is jointly processed with any of these bodies and it is lawful and necessary to do so, the relevant organisations may act as joint controllers.

### 3. The Seven Guiding Principles of Data Processing

The PCC will process personal data in accordance with the seven principles of UK GDPR. Personal data must be:

- i. processed lawfully, fairly and transparently;
- ii. collected for specified and legitimate purposes;
- iii. adequate, relevant and limited to what is necessary;
- iv. accurate and kept up to date;
- v. retained only for as long as necessary;
- vi. processed securely and confidentially;
- vii. and processed in a manner demonstrating accountability.

The PCC will maintain appropriate records of processing activities where required.

### 4. Types of Personal Data we Process

The PCC may process where appropriate:

- i. **General Personal Data** including names and titles; postal addresses; email addresses; telephone numbers; emergency contact details; photographs and video recordings; attendance records; volunteering information; training records; financial and Gift Aid records; church membership and electoral roll information; communications preferences; pastoral notes where appropriate; hall bookings and event participation records; and online identifiers and website usage data.
- ii. **Special Category Data:** because the PCC is a religious organisation, some data processed may reveal religious belief. The PCC may also process safeguarding information; DBS information where lawful; health or accessibility information; dietary requirements; racial or ethnic origin where relevant; biometric images such as photographs; pastoral care information; and where lawful and necessary, other special category data. Special category data will only be processed where a lawful condition applies under Article 9 UK GDPR and Schedule 1 Data Protection Act 2018.
- iii. **Criminal Offence Data:** where authorised by law and necessary for safeguarding or recruitment purposes, the PCC may process DBS and safeguarding-related criminal offence data.

### 5. Lawful Bases for Processing

The PCC relies on one or more of the following lawful bases: consent; legal obligation; legitimate interests; contractual necessity; vital interests; substantial public interest; employment obligations; and processing by a not-for-profit religious body.

- i. Legitimate interests may include pastoral ministry; church administration; safeguarding; volunteer management; maintaining contact with church members; operating church activities safely; fraud prevention; security monitoring; and charity governance.
- ii. Where consent is required, it must be freely given; specific; informed; unambiguous; and capable of withdrawal. Consent records will be maintained where appropriate.

## **6. Children, Young People and Safeguarding**

The PCC recognises that safeguarding responsibilities may require the processing and sharing of sensitive personal data.

- i. Safeguarding processing may include DBS administration; safer recruitment; incident reporting; referrals; safeguarding risk assessments; pastoral support; complaints handling; and liaison with statutory authorities.
- ii. The PCC may share safeguarding information with diocesan safeguarding teams; police; social services; the Charity Commission; insurers; legal advisers; and other agencies where legally required or necessary to protect individuals.
- iii. Children's personal data will receive enhanced protection. Parental consent may be required for: photographs; livestream participation; online groups; communications; trips and activities; and publication of names or images.

The PCC will take reasonable steps to protect children and vulnerable adults from online harms and misuse of personal information.

## **7. Soft Opt-In for Church and Charity Communications**

Where permitted under the Privacy and Electronic Communications Regulations (PECR), the PCC may rely on the 'soft opt-in' exemption to send electronic communications relating to the Church's charitable, pastoral, fundraising, stewardship, campaigning or community activities without obtaining separate explicit consent in every case.

The PCC will only rely on the soft opt-in where all applicable legal conditions are satisfied, including that:

- i. the individual's contact details were obtained during a previous interaction, transaction, donation, event registration, volunteering activity, pastoral contact or other existing relationship with the Church;
- ii. the communications relate to the Church's charitable aims, activities, fundraising or mission and are similar or relevant to the individual's existing relationship with the Church;
- iii. the individual was given a clear opportunity to refuse or opt out of such communications at the time their details were collected;
- iv. the individual is provided with a simple means of opting out in every subsequent communication; and
- v. the individual has not previously objected to or opted out of such communications.

The PCC will maintain suppression and opt-out records to ensure that individuals who opt out do not continue to receive such communications. The PCC will not rely on the soft opt-in where consent is otherwise legally required, where communications are inappropriate to the relationship, or where the rights and freedoms of individuals would override the PCC's legitimate interests.

The PCC recognises that additional care may be required when communicating with children, vulnerable adults or individuals receiving pastoral support.

## **8. Online Safety, Digital Communications and Social Media**

- i. **General Principles:** all digital communications must be lawful; respect confidentiality; comply with safeguarding standards; avoid unnecessary disclosure of personal data; and be conducted professionally.

The PCC recognises responsibilities arising from the Online Safety Act, particularly regarding children, harmful communications and digital risk management;

- ii. **WhatsApp and Other Messaging Platforms**

The use of WhatsApp, Signal, Messenger, SMS or similar platforms must comply with PCC policy.

Requirements include: ministry-related groups must have appropriate oversight; safeguarding guidance must be followed; personal numbers should only be shared where necessary; sensitive pastoral or safeguarding matters should not normally be discussed in informal group chats; administrators must remove users who should no longer have access; users must avoid excessive sharing of personal data; children's and youth groups must follow safeguarding protocols; disappearing-message functions should not be used for safeguarding-related communications; and screenshots or message forwarding must not be used inappropriately.

The PCC reserves the right to require ministry-related communications to be conducted only through approved channels.

- iii. **Email and Marketing Communications**

The PCC will comply with PECR requirements and will: provide unsubscribe mechanisms where required; respect marketing preferences; obtain consent where legally required; avoid unsolicited electronic marketing; and maintain suppression lists where appropriate.

- iv. **Social Media**

The PCC may use social media platforms for ministry, outreach and communication. Content must: be lawful and respectful; avoid bullying, harassment or discrimination; protect confidentiality; avoid identifying children or vulnerable persons without permission; and comply with safeguarding guidance.

Only pre-authorised persons may manage official church accounts.

## **9. Artificial Intelligence (AI) and Automated Tools**

The PCC recognises increasing use of generative AI and automated technologies.

- i. AI tools may only be used where: there is a lawful basis for processing; personal data is minimised; confidential or safeguarding information is not uploaded into public AI systems unless specifically authorised and safeguarded; users understand risks relating to accuracy

and confidentiality; outputs are reviewed by a human decision-maker; and appropriate contracts and safeguards exist.

- ii. The PCC prohibits the use of public AI tools for confidential safeguarding information; DBS information; detailed pastoral records; medical information; or legally privileged material, unless specifically authorised and risk assessed.

The PCC will on an ongoing basis monitor developments in AI regulation and Church guidance.

## **10. CCTV, Photography, Livestreaming and Media**

- i. The PCC may operate **CCTV systems** for: crime prevention; security; safeguarding; protection of property; and investigation of incidents.

Clear signage will be displayed where CCTV operates.

CCTV footage will be securely stored; only accessed by authorised persons; normally be retained for a limited period unless required for investigation; and will only be disclosed where lawful.

- ii. The PCC may **livestream or record services and events**. Reasonable efforts will be made to inform attendees; provide seating outside primary camera areas where practicable; obtain permissions where appropriate; and protect children and vulnerable adults.
- iii. **Photography at church events** should be respectful and proportionate.

## **11. Data Security**

- i. The PCC will decide and implement appropriate technical and organisational storage measures, including password protection; multi-factor authentication where possible; encryption where appropriate; secure cloud storage; secure disposal of records; restricted access permissions; cybersecurity measures; regular software updates; data backup procedures; confidentiality obligations; and volunteer and staff training.
- ii. Where permitted, paper records containing personal data must be stored securely in a manner agreed with the PCC.
- iii. Where permitted, personal data stored on personal devices must be stored securely in a manner agreed with the PCC, and must not be stored indefinitely.
- iv. Lost devices or suspected breaches must be reported to the incumbent, safeguarding officer or PCC Secretary immediately.

## **12. Cloud Storage and Third-Party Providers**

The PCC may use third-party providers including church management systems; cloud storage providers; payroll providers; email systems; livestreaming platforms; donation processors; DBS providers; and website hosting services.

The PCC will seek to ensure that providers offer appropriate security; provide lawful processing arrangements; comply with UK GDPR requirements; maintain appropriate international transfer safeguards where relevant; and process data only on documented instructions.

Written data processing agreements will be used where required.

### **13. International Data Transfers**

Where personal data is transferred outside the United Kingdom, the PCC will ensure appropriate safeguards exist. These may include adequacy regulations; International Data Transfer Agreements; recognised transfer mechanisms; or equivalent lawful safeguards.

Users should recognise that some online platforms may process data internationally.

### **14. Retention of Records**

The PCC will maintain a records retention schedule. Retention periods will reflect legal obligations; safeguarding requirements; insurance requirements; diocesan guidance; charity governance needs; and operational necessity.

Examples may include Gift Aid and financial records (normally at least 7 years); safeguarding records (in accordance with safeguarding guidance and diocesan policy); electoral roll records, as legally required; limited retention for CCTV recordings unless required for investigation; personnel files, according to employment law and safeguarding requirements.

Records no longer required will be securely deleted or destroyed.

### **15. Data Subject Rights**

Individuals have rights under UK GDPR, subject to lawful exemptions.

These include the right to be informed; the right of access; the right to rectification; the right to erasure; the right to restrict processing; the right to data portability; the right to object; and rights relating to automated decision-making.

Requests should normally be answered within one month. The PCC may request proof of identity before responding. Some requests may be limited where legal exemptions apply, including safeguarding, legal privilege, confidential references or ecclesiastical records.

### **16. Subject Access Requests (SARs)**

The PCC will maintain procedures for responding to Subject Access Requests. Requests may be made verbally or in writing. The PCC may verify identity; clarify scope; redact third-party information; refuse manifestly unfounded or excessive requests where lawful; and maintain records of responses.

The PCC will seek legal or diocesan advice where necessary.

### **17. Data Breaches**

- i. A personal data breach includes loss of data; unauthorised disclosure; cyberattack; accidental deletion; ransomware; unauthorised access; or inappropriate sharing.
- ii. All breaches or suspected breaches must be reported immediately to the incumbent, safeguarding officer or PCC Secretary immediately.

- iii. The PCC will: investigate incidents; assess risk; maintain breach records; notify the Information Commissioner's Office where legally required; and notify affected individuals where there is a high risk to rights and freedoms. The PCC will maintain an internal breach response process.

## 18. Complaints Handling Procedure

The PCC is committed to handling complaints fairly, promptly and transparently.

Complaints relating to privacy, data protection or information governance may concern misuse of personal data; inappropriate disclosure; safeguarding concerns; online conduct; CCTV use; direct marketing; failure to respond to requests; confidentiality breaches; or information security concerns.

- i. **How to Make a Complaint:** complaints may be made by email; in writing; by telephone; or in person. Complaints should normally include: the complainant's name and contact details; details of the concern; dates and persons involved where known; and desired outcome.
- ii. **Complaint Handling:** the PCC will: acknowledge complaints promptly; investigate fairly and confidentially; keep appropriate records; seek safeguarding advice where required; respond within a reasonable period; and explain any further escalation routes.
- iii. **Escalation:** individuals may complain to the Diocese of Chichester where relevant; the Information Commissioner's Office; the Charity Commission; safeguarding authorities; or other regulatory bodies.

The Information Commissioner's Office can be contacted at:

Information Commissioner's Office  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire SK9 5AF  
Telephone: 0303 123 1113  
Website: <https://ico.org.uk/>

## 19. Training and Responsibilities

The PCC is collectively responsible for ensuring compliance. With the incumbent, churchwardens and relevant officers, they must ensure appropriate governance; confidentiality; safeguarding integration; staff and volunteer awareness; and incident reporting.

Appropriate training should be provided for: safeguarding officers; pastoral teams; livestream and media volunteers; administrators; PCC members; and anyone handling personal data.

Failure to comply with this PCC policy may result in disciplinary or safeguarding action.

## **20. Review of Policy**

This policy will be reviewed annually; following significant legal or regulatory change; after major incidents or breaches; or following significant operational changes.

## **21. Contact Details**

Questions, concerns or requests relating to this policy should be addressed to:

The PCC Secretary of Holy Trinity Church Cuckfield  
The Church Office  
The Old School  
Church Street  
Cuckfield  
West Sussex RH17 5JZ

Email: [office@holytrinitycuckfield.org](mailto:office@holytrinitycuckfield.org)  
Telephone: 01444-456461