



FREE GUIDE · DATA AND COMPLIANCE

Church GDPR Checklist

A comprehensive GDPR compliance checklist for UK churches covering data handling, consent, breaches and ICO registration.

We try hard to get everything here right, and every guide and template shows when it was last reviewed. But they are free, they are general and things change: the law, prices and the tools themselves. We cannot guarantee they are complete, current or right for your church, so check anything you rely on and take professional advice where a decision matters.

Church GDPR Checklist

Who this is for: the church council or trustees responsible for how the church handles people's data, and the person who has been asked to check it is done properly.

Introduction

Data protection can feel overwhelming, but for most churches it comes down to common sense and good record-keeping. This checklist is designed to help your church council or trustees make sure you are meeting your obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

This is not legal advice. For complex situations, consult your denominational data protection officer or seek professional guidance. But for the everyday data handling that most churches do, this checklist will help you get the basics right.

Key references:

- ICO (Information Commissioner's Office): ico.org.uk
 - ICO guidance for charities: ico.org.uk/for-organisations/charity
 - Charity Commission guidance (England and Wales): gov.uk/government/organisations/charity-commission
 - OSCR, the Scottish Charity Regulator: oscr.org.uk
 - Charity Commission for Northern Ireland: charitycommissionni.org.uk
-

1. Who Is the Data Controller?

The data controller is the organisation legally responsible for how personal data is used. In a church context, this is usually the governing body, not an individual.

- ☐ We have identified our data controller (e.g. PCC, church council, board of trustees, managing trustees)
- ☐ We understand that the data controller is legally responsible for compliance, not the minister or administrator alone
- ☐ We have a named person who takes the lead on data protection matters (this does not have to be a formal Data Protection Officer for most churches, but someone needs to own it)
- ☐ Our data controller is recorded in relevant policies and privacy notices

Common examples:

Denomination	Typical Data Controller
Church of England	The PCC (Parochial Church Council)
Methodist Church	The managing trustees of the local church
Baptist churches	The trustees or church meeting
Catholic parishes	The diocese (parish priest acts on behalf of the diocese)
URC	The elders' meeting or church meeting
Church of Scotland	The Kirk Session (the minister and elders) with any separate Congregational or Financial Board; the Church's own guidance says a congregation can have more than one controller, so check with your Presbytery
Scottish Episcopal Church	The Vestry
Church in Wales	The Ministry Area Council in most Ministry Areas
Church of Ireland	The parish, acting through its Select Vestry
Presbyterian Church in Ireland	The congregation, acting through its Kirk Session

Check your denomination's specific guidance, as structures vary.

Scotland, Wales and Northern Ireland

In England and Wales many churches are 'excepted' charities: a charity in law, but not required to register with the Charity Commission unless income is over £100,000. The exception is due to end in 2031.

UK GDPR, the Data Protection Act 2018 and the ICO fee apply across the whole of the UK, so the data protection sections of this checklist do not change by nation. The charity side does.

Scotland. There is no excepted status. Every body that calls itself a charity in Scotland must be on the Scottish Charity Register, held by OSCR, whatever its income. From 9 March 2026 OSCR publishes the first and last names of every charity trustee on the charity's Register entry, and publishes submitted accounts in full. That is personal data about your Kirk Session, Vestry or trustees going into the public domain, so say so in your privacy notice and tell people before they are appointed. Serious matters go to OSCR through its raise a concern form; the old Notifiable Events process ended on 1 April 2024.

Wales. The Charity Commission and the excepted-charity rules are the same as in England. The Church in Wales is disestablished and has its own structures: in most places the Ministry Area

Council is the data controller, and the Representative Body, which holds the Church's assets, issues its central privacy notices.

Northern Ireland. Registration with the Charity Commission for Northern Ireland is compulsory for every charity, however small, and there is no excepted-church category. The Commission calls organisations forward in stages, and paused new invitations in 2026 while it upgrades its systems, so check your church's current status on the CCNI register before you write it into a privacy notice. Serious incidents are reported to CCNI under its own guidance for trustees. The Presbyterian Church in Ireland and the Methodist Church in Ireland both span the border, so a congregation's regulator depends on which side of it the congregation sits.

2. Lawful Basis for Processing

Under UK GDPR, you need a lawful basis for every type of personal data you process. The two most relevant for churches are **legitimate interests** and **consent**.

Legitimate Interests

- ☐ We use legitimate interests where appropriate (e.g. maintaining a membership list, contacting members about church activities, managing volunteers)
- ☐ We have documented our legitimate interests assessment (a brief record of why our interest outweighs the individual's privacy rights)
- ☐ We understand that marketing by email or text needs PECR consent (or the narrow charity soft opt-in) whoever the recipient is, and that legitimate interests alone is not enough

Consent

- ☐ We use consent where required (e.g. adding someone to a mailing list, publishing their photograph, sharing their data with third parties)
- ☐ Our consent requests are clear, specific and separate from other terms
- ☐ We keep records of when and how consent was given
- ☐ We make it easy for people to withdraw consent at any time
- ☐ We do not use pre-ticked boxes or assume consent from silence

Special Category Data

Churches often process special category data (religious belief, health information, ethnicity). Extra protections apply.

- ☐ We have identified where we process special category data

- ☐ We have an appropriate lawful basis and condition for processing (for religious organisations, this is usually "processing by a not-for-profit body with a religious aim" under Article 9(2)(d), but only for members and those in regular contact)
 - ☐ We have an appropriate policy document in place (the Data Protection Act 2018 requires one when you rely on the substantial public interest or employment conditions for special category data, and for criminal offence data such as DBS results; your denomination may publish a model one)
-

3. Church Membership Rolls

- ☐ Our church membership roll contains only the data we need (name, address and any other required fields)
- ☐ We review the roll regularly and remove people who are no longer members
- ☐ The roll is stored securely (physical copies locked away, digital copies password-protected)
- ☐ Access to the roll is limited to those who need it
- ☐ We understand any denomination-specific legal requirements for our membership roll

Church of England specific: The electoral roll must be revised annually and renewed every six years. There are legal requirements for public display of the electoral roll – consider displaying names only, not addresses, where possible under church law.

4. Mailing Lists and Newsletters

Email newsletters and postal mailings are covered by both UK GDPR and the Privacy and Electronic Communications Regulations (PECR).

Email and Electronic Communications

- ☐ We have consent from every person on our email mailing list
- ☐ Consent was freely given, specific and informed (not assumed from church attendance)
- ☐ Every email includes a clear and working unsubscribe link
- ☐ We process unsubscribe requests promptly (within a few days at most)
- ☐ We keep a record of how and when each person subscribed
- ☐ We do not add people to the mailing list without their explicit permission
- ☐ We use a reputable email platform (e.g. Mailchimp, beehiv) rather than CC/BCC in regular email

Postal Communications

- ☐ We have a lawful basis for sending postal mailings (consent or legitimate interests)

- ☐ We give people the option to opt out of postal communications
- ☐ Our mailing list is kept up to date (no letters to people who have moved away or asked to stop)

Key PECR Points

- PECR requires consent for unsolicited marketing emails. ⚠️ Since 5 February 2026 there is a narrow charity exception – see the DUAA section below – but it does not apply to details you collected before then
 - Church newsletters that include fundraising appeals or event promotions may count as marketing
 - Transactional or purely administrative emails (e.g. rota reminders) are less likely to require PECR consent, but good practice is to have consent anyway
-

5. Photography and Video

- ☐ We have a clear photography and video policy
 - ☐ We display notices at services and events informing people that photography or filming may take place
 - ☐ We obtain specific consent before photographing or filming individuals for use on websites, social media or publications
 - ☐ We have parental or guardian consent before photographing or filming children (under 18)
 - ☐ Our consent forms specify where images will be used (website, social media, printed materials, local press)
 - ☐ We review and delete images when consent is withdrawn or when they are no longer needed
 - ☐ We do not publish images of children alongside their full names
 - ☐ We have considered whether livestreaming services requires additional consents
 - ☐ We brief anyone taking photographs at events about our policy
-

6. Website Privacy Policy and Cookies

Your church website must have a privacy policy. If it uses cookies (and almost all websites do), you need a cookie notice too.

Privacy Policy

- ☐ Our website has a privacy policy that is easy to find (linked in the footer of every page)
- ☐ The privacy policy states who the data controller is
- ☐ It explains what personal data we collect through the website (e.g. contact forms, newsletter sign-ups, donation forms)

- ☐ It explains why we collect this data and our lawful basis
- ☐ It explains how long we keep the data
- ☐ It explains people's rights (access, correction, deletion, complaint to the ICO)
- ☐ It includes contact details for data protection queries
- ☐ It has been reviewed in the last 12 months

Cookies

- ☐ Our website displays a cookie consent banner that allows users to accept or reject non-essential cookies
- ☐ We do not load non-essential cookies (analytics, social media embeds, advertising) until the user consents
- ☐ We have a cookie policy that lists the cookies used, their purpose and their duration
- ☐ We review our cookies periodically (plugins and themes can add new cookies without you realising)

7. Subject Access Requests

Any person has the right to request a copy of the personal data you hold about them. This is called a Subject Access Request (SAR).

Stop before you search: does this touch a safeguarding record?

If the requester is, or may be, the subject of a safeguarding concern, do not process the request yourself. Hand it to your safeguarding lead and your denominational data protection officer before you look anything up.

Followed literally, the process below would disclose a safeguarding file to the person the concern is about – including who raised it and, often, a child's own words. That has exposed children and reporters to serious harm in real cases.

The exemptions exist for exactly this. Data may be withheld where disclosure would be likely to prejudice safeguarding, prevention or detection of crime, or would reveal a third party who has not consented. **Deciding which applies is a job for your DPO, not a volunteer with a deadline.**

The right to erasure does not apply to safeguarding records. Never delete a safeguarding record because someone asked you to – not even the person it concerns.

Where to go for safeguarding advice. Nothing on this site is safeguarding guidance and we do not write any. Your denomination's safeguarding policy and its safeguarding team are the

authority, and they take precedence over anything here. For independent advice, [thirtyone:eight](#) runs a helpline for churches on 0303 003 1111; the NSPCC Helpline is 0808 800 5000. Allegations against an adult working with children go to your local authority LADO. If a child or adult is at immediate risk, call 999.

- ☐ We know how to recognise a SAR (it does not have to use formal language – "Can you tell me what information you have about me?" counts)
- ☐ We have a process for responding to SARs
- ☐ We know the deadline: one calendar month from receipt
- ☐ We know we cannot charge a fee for most SARs
- ☐ We can verify the identity of the requester before releasing data
- ☐ We know where all personal data is held (paper files, email, databases, cloud services) so we can search comprehensively
- ☐ We understand that we may need to redact third-party data before releasing information

If you receive a SAR and are unsure how to respond, contact your denominational data protection officer or the ICO helpline (0303 123 1113) promptly. Do not ignore it or delay.

8. Data Breach Procedure

A data breach is any incident where personal data is accidentally or unlawfully lost, stolen, destroyed or disclosed to someone who should not have it.

Examples of Church Data Breaches

- Emailing the membership roll to the wrong person
- Leaving a printout of pastoral notes on a train
- A laptop containing church records being stolen
- Accidentally sending an email with all recipients visible in the "To" field instead of "BCC"
- A church officer discussing a safeguarding concern with someone not involved

Your Breach Procedure

- ☐ We have a written data breach procedure that all key volunteers and staff know about
- ☐ We know we must assess every breach to determine risk to individuals
- ☐ We know we must report serious breaches to the ICO within **72 hours** of becoming aware (ico.org.uk/for-organisations/report-a-breach/ – note this is the route for organisations. The [make-a-complaint](#) pages are for members of the public complaining *about* an organisation and give you no way to file a breach report)

- ☐ We know we must inform affected individuals without undue delay if the breach is likely to result in a high risk to their rights
- ☐ We keep a log of all data breaches, even minor ones, recording what happened, the data involved and what action was taken
- ☐ We know who in our church is responsible for managing a breach (this should be the data protection lead or a named trustee)

⚠️ One incident, up to three reports

Look again at the last example above – *a church officer discussing a safeguarding concern with someone not involved*. That single act is:

1. a **data breach**, which may need reporting to the **ICO** within 72 hours;
2. a **safeguarding incident**, which goes to your safeguarding lead and may need reporting to the local authority; and
3. potentially a **Serious Incident**, which charities in England and Wales must report promptly to the **Charity Commission**, whether registered or excepted; the trustees are responsible for the report.

In Scotland the route is OSCR's raise a concern form; in Northern Ireland it is a serious incident report to the Charity Commission for Northern Ireland.

Charity Commission Serious Incident Reporting is the one churches forget. It covers safeguarding incidents, significant financial loss or fraud, and serious data breaches. The Commission has been explicit that it takes a much dimmer view of a failure to report than of the incident itself, and reporting is a **trustee** duty – it does not discharge by telling the minister.

Write all three routes into your breach procedure now, while nothing has happened. Nobody works out a three-way reporting obligation calmly on the day.

9. Children's Data

Children's personal data has extra protections under UK GDPR. The UK sets the age of digital consent at 13, but for church activities, extra care is needed regardless of age.

- ☐ We collect only the minimum data needed about children (name, age, emergency contact, medical/dietary needs for activities)
- ☐ We obtain consent from a parent or guardian before processing children's data
- ☐ We store children's data securely and separately from general church records where possible
- ☐ We do not share children's data with third parties without parental consent

- ☐ We follow our denomination's safeguarding data handling requirements
- ☐ Our privacy notice covers how we handle children's data
- ☐ We delete **routine** children's data when it is no longer needed – registers, dietary and medical notes, emergency contacts – typically at the end of the activity year after the child leaves
- ☐ **We never delete anything connected to a safeguarding concern on this basis.** Records of concerns, allegations or referrals are kept in line with denominational policy – often indefinitely, and often to national retention standards set after IICSA. If in doubt, keep it and ask your safeguarding lead, or thirtyone:eight on 0303 003 1111 (see the box in section 7)

Why the distinction matters. A child who was harmed may not disclose for twenty or thirty years. The [Independent Inquiry into Child Sexual Abuse](#) found that some of the records it needed were "simply missing" and others "had been destroyed in accordance with retention policies in place at the time", and recommended that records known to relate to allegations of child sexual abuse be kept for 75 years (Recommendation 17). "We deleted it under GDPR" is not a defence; UK GDPR has never required it.

10. Volunteer and Staff Data

If your church has employees or manages volunteers, you are processing their personal data too.

- ☐ We have a privacy notice for staff and volunteers (separate from the general church privacy notice)
- ☐ We collect only the data we need (contact details, DBS check status, role, emergency contact)
- ☐ DBS certificate information is stored securely and access is restricted to those who need it
- ☐ **We do not keep copies of DBS certificates.** The DBS Code of Practice position is not to retain a copy at all; where one is kept for a specific, justified reason, it is destroyed within six months of the recruitment decision
- ☐ **We do keep a permanent record of each check** – this is a different thing from the certificate, and it must survive: certificate number, level of check (Basic / Standard / Enhanced / Enhanced with Barred List), date of issue, the position it was for and the recruitment decision that was made

Don't destroy the audit trail while destroying the certificate. These are two different records and only one of them should go. A Charity Commission inquiry, an insurer or a denominational audit will ask you to evidence *that* someone was checked, at what level and what you decided. If you have shredded the certificate and kept no record, you cannot answer – and the honest answer sounds identical to never having checked at all.

- ☐ We keep personnel and volunteer records secure (locked filing cabinet, password-protected files)

- ☐ We have a clear retention period for staff and volunteer records
- ☐ We inform volunteers and staff about how their data is used

11. Sharing Data with Your Denomination

Most churches share some data with their wider denominational structure. This is usually legitimate and expected, but should be handled properly.

- ☐ We know what data we share with our denomination (e.g. membership numbers, membership roll, safeguarding referrals, financial returns)
- ☐ We have a lawful basis for each type of data sharing
- ☐ Our privacy notice mentions that data may be shared with the wider denomination and for what purposes
- ☐ We understand any data sharing agreements our denomination has in place
- ☐ We do not share more data than is necessary for the stated purpose
- ☐ We use secure methods to transfer data (not unencrypted email attachments containing personal details)

12. Record Retention

You should not keep personal data longer than you need it. But some records must be kept for specific periods.

Suggested Retention Periods

Record Type	Suggested Retention Period	Notes
Registers of services (baptisms, marriages, burials)	Permanently	Legal and historical records
Church council/trustee meeting minutes	Permanently	Governance records
Financial records and accounts	6 years from the end of the financial year	Charities Act 2011, s.131
Gift Aid declarations	6 years after the end of the tax year of the last claim; enduring declarations kept for as long as you rely on them	HMRC - HMRC recovers unevidenced claims from the church, not the donor
Membership roll	Until next revision/renewal	Check denomination-specific requirements

Record Type	Suggested Retention Period	Notes
General correspondence	3 years	Unless relevant to ongoing matters
Employment records	6 years after employment ends	Limitation period for claims
DBS certificates (the copy)	Do not retain; 6 months maximum if justified	DBS Code of Practice
DBS record of check (number, level, date, position, decision)	Permanently	Audit and safeguarding evidence – do not destroy with the certificate
Safeguarding records	Follow denominational policy	Often indefinite due to nature of concerns
Event sign-up sheets	1 year	Delete after the event cycle
Mailing list consent records	Duration of subscription + 1 year	In case of dispute
Photographs	Review every 5 years	Remove if consent withdrawn or no longer needed

- ☐ We have a written retention schedule
- ☐ We review and delete records according to our schedule at least annually
- ☐ We securely destroy records when they reach the end of their retention period (shredding for paper, secure deletion for digital)

13. The Five Obligations Churches Most Often Miss

Everything above concerns how you *handle* data. These five are things the law requires you to *have*, and most churches have none of them. They are not onerous – between them they are an afternoon's work – but their absence is exactly what an ICO enquiry finds first.

13.1 A Record of Processing Activities (ROPA)

A written list of what personal data you hold, why, on what lawful basis, who you share it with and how long you keep it.

Churches cannot use the "fewer than 250 staff" exemption. That exemption falls away where processing involves **special category data** – and data revealing religious belief is special category data. A church membership roll is a list of people's religion. **You are in scope.**

- ☐ We have a written ROPA covering every system that holds personal data

- ☐ It names, for each: the data, the purpose, the lawful basis, who it is shared with, where it is stored and the retention period
- ☐ It includes the informal systems too – the WhatsApp groups, the spreadsheet on the treasurer's laptop, the rota app someone set up
- ☐ We review it annually and when we start anything new

13.2 Data Protection Impact Assessments (DPIAs)

A DPIA is a short written assessment done **before** starting something higher-risk. Churches have two classic triggers and usually do both without one:

- **Livestreaming** – systematic monitoring of a publicly accessible space, capturing children and adults at risk, publishing religious belief
 - **CCTV** – the same monitoring test, and it goes unmentioned in most church data policies
- ☐ We have completed a DPIA for our livestream, if we stream
 - ☐ We have completed a DPIA for any CCTV, and there is a sign saying who operates it and why
 - ☐ We do a DPIA before adopting any new system that profiles people, tracks them, or processes children's or health data
 - ☐ Where a DPIA shows a high risk we cannot reduce, we know we must consult the ICO before going ahead

13.3 Contracts With Your Processors (Article 28)

Anyone who handles personal data **on your instructions** is a processor: your church management software, your mailing list provider, your website host, your accountant, your cloud storage. UK GDPR requires a written contract with each one, containing specific terms.

- ☐ We have listed every processor we use
- ☐ Each has a written contract or data processing agreement in place (for most cloud services this is their standard DPA – you usually need to accept it, not negotiate it)
- ☐ We have checked that each is actually signed up to, not merely offered
- ☐ We do not let a volunteer sign up the church to a new tool without this check

13.4 International Transfers (Chapter V)

If your provider stores data outside the UK, that is a restricted transfer and needs a legal mechanism – usually adequacy, or the UK's International Data Transfer Addendum.

- ☐ We know where each provider stores our data
- ☐ Our privacy notice tells people if their data leaves the UK
- ☐ For any provider outside a country with UK adequacy, we have the addendum in place

13.5 The Data (Use and Access) Act 2025

The DUAA received Royal Assent in June 2025, with most provisions commencing through 2026. Two parts matter to churches:

- **A statutory complaints duty, in force since 19 June 2026.** If someone complains to you about how you handle their data, you must **facilitate** the complaint – the Act names providing a complaint form that can be completed electronically – **acknowledge it within 30 days**, and respond without undue delay. Most church privacy notices do not mention complaints at all, and an email address alone is thin compliance.
 - **A charity soft opt-in.** Charities may email people whose details they obtained when those people expressed an interest in, or offered support to, the charity's purposes – without fresh consent, subject to conditions. Broadly the allowance commercial organisations have had for years. It is genuinely helpful, and it is narrower than it sounds in three ways worth knowing before you rely on it:
 - **⚠ It is not retrospective, so your existing list almost certainly does not qualify.** The provision requires that the person was given a simple means of refusing marketing **at the time their details were first collected** (PECR reg 22(3A)(c)). A list gathered before February 2026 without that refusal route at the point of collection cannot meet the condition. Treat this as a rule for people you sign up from now on, not a licence to email the people you already have. The same provision requires that refusal route again **in every subsequent message**, so an unsubscribe link in each email is part of the condition and not just good manners.
 - **⚠ The marketing must further the charitable purposes, and only those.** It does not cover selling a product or a service.
 - **⚠ "Charity" is defined differently across the UK.** In England and Wales it is the Charities Act 2011 s.1(1) definition, which **includes excepted charities** – so a PCC or a local Methodist church counts without being registered. In **Scotland** the definition is a body **entered in the Scottish Charity Register**, so registration is required there. Northern Ireland follows its own Act.
 - Every message must still carry an easy unsubscribe, every time.
 - ☐ Our privacy notice says how to complain to us, and names who receives complaints
 - ☐ We can acknowledge a data complaint within 30 days
 - ☐ We have checked whether the charity soft opt-in applies before relying on it
-

14. Annual Data Audit Checklist

Run through this checklist once a year and bring the results to a church council or trustees meeting.

How long this really takes. The *checklist* takes an hour. The *work it uncovers* – chasing consents, tracking down who still has access to what, writing a retention schedule you don't yet have – is

realistically a day or two the first time, and a couple of hours a year after that.

We would rather tell you that than have you block out an hour, discover the size of it and abandon the whole thing. **Do it in pieces.** Take two or three lines to each leadership meeting rather than the lot to one. Nobody has ever completed this list in a single sitting.

- ☐ Review the church membership roll for accuracy
- ☐ Check mailing lists – remove anyone who has unsubscribed or is no longer in contact
- ☐ Review and update the church privacy notice (website and any printed version)
- ☐ Check that the website cookie consent mechanism is working correctly
- ☐ Review who has access to personal data (email accounts, databases, filing cabinets) and remove access for anyone who no longer needs it
- ☐ Check that DBS records are being stored and disposed of correctly
- ☐ Review photograph and video consents – are all published images covered by current consent?
- ☐ Check that data breach log is up to date (even if there have been no breaches, record that fact)
- ☐ Review any data sharing with third parties (denomination, contractors, cloud services)
- ☐ Confirm that all church devices with personal data have passwords or PINs
- ☐ Check that volunteers handling personal data understand their responsibilities
- ☐ Review the data retention schedule and delete anything past its retention date
- ☐ Confirm ICO registration is current (see below)
- ☐ Review the ROPA and add anything new started during the year
- ☐ Confirm every processor still has a data processing agreement in place
- ☐ Check whether anything new needs a DPIA
- ☐ Update this checklist with any new data processing activities started during the year
- ☐ Record the date of this audit and any actions arising in your church council or trustees meeting minutes

15. ICO Registration

Most organisations that process personal data must register with the Information Commissioner's Office and pay an annual data protection fee.

Do Churches Need to Register?

Usually, yes. Most churches process personal data and are therefore required to register. The fee is tiered:

Tier	Who it covers	Fee
Tier 1 (Micro)	Turnover up to £632,000, or no more than 10 staff	£52/year
Tier 2 (Small/Medium)	Turnover up to £36 million, or no more than 250 staff	£78/year
Tier 3 (Large)	Everyone who does not meet tier 1 or tier 2	£3,763/year

If your church is a charity, registered or excepted, you pay the tier 1 fee (£52) whatever your size or turnover. That is a specific concession in the regulations, and it, not your size, is why nearly every church pays £52. A large church with several staff and a six-figure turnover still pays £52 if it is a charity. (In Scotland the church must be on the Scottish Charity Register; in Northern Ireland it must be a charity under the 2008 Act.)

Pay by direct debit and the ICO takes £5 off automatically – £47 rather than £52. There is no reason not to.

Exemptions: A not-for-profit body that processes data only to keep membership and supporter records, run its own activities for members and regular contacts, and keep its accounts *maybe* exempt. Paid staff do not, on their own, take you outside it. However, most churches do more than this (mailing lists, photography, DBS checks, sharing data with denominations), so the exemption rarely applies in practice.

Fees checked against ico.org.uk in August 2026. The ICO sets these by statute and they do change – check before you budget.

- ☐ We are registered with the ICO (or have confirmed we are exempt)
- ☐ Our registration is renewed annually
- ☐ Our registration details are correct and up to date
- ☐ We know our ICO registration number

Check or register at: ico.org.uk/for-organisations/data-protection-fee

Quick Reference: Key Rights of Individuals

People whose data you hold have the following rights. You should be prepared to respond to any of these:

1. **Right to be informed** – they must know what data you hold and why (your privacy notice covers this)
2. **Right of access** – they can request a copy of their data (Subject Access Request)
3. **Right to rectification** – they can ask you to correct inaccurate data
4. **Right to erasure** – they can ask you to delete their data (with some exceptions)

5. **Right to restrict processing** – they can ask you to limit how you use their data
 6. **Right to data portability** – they can ask for their data in a portable format
 7. **Right to object** – they can object to processing based on legitimate interests
 8. **Rights related to automated decision-making** – not usually relevant for churches
-

Useful Contacts and Resources

- **ICO helpline:** 0303 123 1113 (Monday to Friday, 9am to 5pm)
- **ICO website:** ico.org.uk
- **ICO guidance for charities:** ico.org.uk/for-organisations/charity
- **Charity Commission (England and Wales):** gov.uk/government/organisations/charity-commission
- **OSCR (Scotland):** oscr.org.uk
- **Charity Commission for Northern Ireland:** charitycommissionni.org.uk
- **Church of England resources:** parishresources.org.uk
- **CCLI (for music licensing, not data, but often confused):** ccli.com

Check your denomination's website for denomination-specific data protection guidance and template documents.

Sources

The nation-specific claims in this guide were checked against the pages below on 5 September 2026. ICO fees carry their own check date in section 15. Prices and product names change; the date at the top of the guide says when they were last confirmed. Claims that rest on pages we could not reach at the time of checking are not listed.

- **No excepted charities in Scotland:** [Registration: cross-border charity regulation in Scotland](#). Confirms that all organisations representing themselves as charities in Scotland must register with OSCR and that there are no exempt or excepted categories.
- **OSCR publishes trustee names and full accounts:** [More information to appear on the Scottish Charity Register from 9 March 2026](#). Confirms that trustees' first and last names appear on the Register entry and that accounts submitted from 9 March 2026 are published in full.
- **OSCR reporting route:** [The Notifiable Events process has been replaced](#). Confirms the change on 1 April 2024 and the raise a concern form as the route for unresolved serious issues.
- **Excepted churches in England and Wales:** [Excepted charities](#). Confirms that churches linked to the listed denominations are excepted from registration while their income is £100,000 or less, that the exception ends in 2031 and that excepted charities must still comply with charity law.

- **Compulsory registration in Northern Ireland:** [Registration](#). Confirms that every charity must register however small, that organisations are invited in stages and that invitations are paused during a systems upgrade.
- **Serious incident reporting across the three regulators:** [Reporting to charity regulators](#). Confirms the Charity Commission, OSCR and CCNI routes side by side.
- **Church of Scotland congregations:** [Charity trustees, liabilities and OSCR](#), a Church of Scotland circular republished by Pathhead Parish Church. Confirms that a congregation's charity trustees are the minister and the elders on the Kirk Session, plus the members of any separate Financial Board.
- **Scottish Episcopal Church vestries:** [Vestry responsibilities: governance, accounting and charity matters](#). Confirms vestry members act as charity trustees under the Scottish Charities Acts and file an annual return with OSCR.
- **Church in Wales structure:** [About us](#) and [Structure](#). Confirm the Representative Body's role in holding the Church's assets and the Ministry Area as the local unit. The Ministry Area Council as data controller is taken from a published Ministry Area privacy notice: [Merthyr Tydfil Ministry Area](#).
- **Disestablishment:** [Church in Wales](#). Confirms the province was created in 1920 on the disestablishment of the four Welsh dioceses.
- **Church of Ireland select vestries:** [Parish governance](#). Confirms every parish has a Select Vestry that manages its money and buildings.
- **Presbyterian Church in Ireland:** [Presbyterian Church in Ireland](#). Confirms the Kirk Session is the governing body of each congregation and that the Church's congregations sit in both jurisdictions.
- **Methodist Church in Ireland:** [Methodist Church in Ireland](#). Confirms the Church extends across the whole island.