Continue

The diocese of gloucester academies trust

The Diocese of Gloucester Academies Trust is a multi-academy trust that prioritizes children's needs in its decision-making process. This trust is formed by several schools collaborating on strategic initiatives to maintain high educational standards. DGAT has established itself as an effective MAT with a proven track record of supporting schools in improving their services for the benefit of their students. The trust was set up in 2012 to provide a platform for Church of England schools to join, and it has since welcomed a community school into its fold. The trust welcomes inquiries from schools interested in exploring membership opportunities. DGAT's primary goal is to offer inclusive, aspirational, and caring education to children of all faiths or none. This approach ensures that each school maintains its unique character while benefiting from collective strengths. The trust empowers local governance, allowing schools to make decisions on curriculum and teaching methods at their own level. As the trust grows, it provides centralized services and outsourced functions to free up resources for teaching and learning. DGAT believes that by combining individual school strengths with collaborative efforts, they can unlock each child's potential. Our family at Dursley CofE Primary Academy is built on the foundation of blessings. With every blessing,Canon Rachel Howie – Chief Executive Officer. We are stronger togetherFor further information regarding DGAT please click on the link below. DGAT address: 3 College GreenGloucester GL12LR Telephone number: 01452 835572 The Diocese of Gloucester Academies Trust (DGAT) is a family of schools established by the Diocesan Board of Education (DBE) in 2012. The Trust is part of the wider family of Church of England schools in the Diocese of Gloucester. More information about Diocesan Schools can be found here. Our purpose is to provide children of all faiths and none, with excellent educational provision which transforms lives within a caring and supportive Christian ethos. Our family of schools is fully inclusive and welcoming to all. There are currently 22 primary schools and two infant schools within the Trust. Twenty-two of the twenty-four schools have a religious designation as Church of England schools. All of the schools are located in Gloucestershire Local Authority. Supporting children's spiritual, moral, social, cultural and physical development, and maximizing their progress, achievement, and attainment to ensure their intellectual growth is key. In tandem with this is the drive to support and develop the staff within our family of schools. To build strong learning communities, we ensures that schools are confident and outward-facing in all they do, building strong, effective links with parents, parishes, local schools, community groups and the wider educational community. The Trust has a high level of expertise in school improvement at a central level and within individual schools. This is used to support schools on their journey towards outstanding. We're looking for a dedicated teacher to join our team at Longney CofE Primary Academy. The ideal candidate will share our vision, be passionate about transforming lives through quality teaching, and thrive in a nurturing environment. If you're ready to take your career to the next level and make a difference, we'd love to hear from you. We're seeking two After School Club Leaders to join us on a fixed-term contract. As an After School Club Leader, you'll be responsible for developing and overseeing high-quality play experiences, ensuring smooth day-to-day operations, and prioritizing child safety and well-being. In return, we offer a positive work environment, flexible working hours, and opportunities for professional growth. The successful applicant will be expected to complete an enhanced DBS disclosure as part of our safeguarding commitment. The application deadline is Friday, 2nd May 2025, with the start date to be confirmed upon selection. Administrator and Attendance Officer Wanted at Hatherley Infants School The Diocese of Gloucester Academies Trust is seeking a motivated individual to fill a part-time School Administrator and Attendance Officer role at Hatherley Infants School. The ideal candidate will have strong organizational skills, be detail-oriented, and possess excellent communication abilities. As the Administrator and Attendance Officer, you will play a crucial role in supporting the efficient operation of the school by accurately managing attendance records and handling various administrative tasks. This part-time position offers 19.5 hours per week, with a salary of £11,390 (pro-rata) based on experience. To apply, please visit our website for further details and application forms. The successful candidate will be required to complete an enhanced DBS disclosure as part of the hiring process. The Diocese of Gloucester Academies Trust is committed to safeguarding and promoting the interests of children and young people. Given text: consider our schools as an extension of our worshipping communities but these regulations appear to work in precisely the opposite direction. Will church schools receive explicit advice about the implementation of the GDPR? Are the downloadable forms on the Diocese website going to be amended so that people can opt out of sharing information with any other body / organisation? E.g. after gift aid receiving requests from charitable organisations for money. We often send out named invitations to the whole village to attend special services. Can we do this without specific permission? Can the Church discuss in person with parishioners who are not necessarily regular church attenders about the Parish Giving scheme? Do we keep copies of personal details forms and confidential declaration forms once an applicant has had a DBS check done? When do we not need consent to process special categories of personal data (such as information about religion)? Can parents give consent on behalf of their children for GDPR purposes? I have contact details for family members which I have obtained through funerals, weddings, baptisms and so on. Do I need consent before I contact them about events? Also, do I need consent before sharing their contact details with other vicars? What does “consent” really mean in practice? Does it have to be in writing? Also, can consent be implied (for example, we have been sending parishioners newsletters for years, can we treat it as valid consent if they have never opted-out or complained)? I understand that under data protection law we need to make sure that the personal data we have is kept secure. This is not something I have thought about before. Where do I start with this? I need to a enter a password before I can access the start screen on my laptop. Does this count as encryption? I would like to include photographs of a recent event in the parish newsletter. Do I need to get consent for this? We have lost a laptop containing staff and payroll information. The laptop also contained scanned copies of staff employment contracts. The laptop was not encrypted. Do we need to tell anyone? I have heard a lot in the news about cyber threats and organisations being hacked. Is this relevant to our parish? I notice in the ‘Consent, Right and Accountability’ of the ‘A Brief Guide to Data Protection for PCC Members’ that from May 2018 people will need to give their consent before we send marketing communications. We send a Benefice Magazine to every household in the benefice which advertises Benefice Church events and also has advertisements from local or relevant traders. Should we be getting consent to deliver this before we push them through peoples letterboxes? Is there anything extra we need to be thinking about when we use contractors to handle personal data. For example, IT contractors? Under the GDPR individuals have a “right to be forgotten”, ie a right to have their personal data deleted. We have some historic information relevant to an allegation made against a former clergy person. Can that individual exercise their right to be forgotten and require us to delete their personal data? Our staff and volunteers use their personal laptops for parish matters. Is this compliant? A local charity has contacted us because they are looking for volunteers. We think that a number of our own volunteers would be a good fit for the charity. Can we pass on their details to the charity? I would like to collect Can we share personal data about parishioners without their consent? Are there specific rules for using memory sticks to store information, and can we keep data for historical research purposes? What about sharing volunteer rota details with other volunteers or contacting people with Church news and events? How do the Data Protection Act implications affect our practice. You should establish a data sharing agreement between parishes that outlines the rules for sharing personal data, including who is responsible for the privacy notice and consent form, how complaints are handled, and data sharing procedures. This agreement doesn't need to be formal; an email exchange or a signed letter can suffice as long as it covers all key points. The data controller is the person or organization legally responsible for data protection compliance, often more than one depending on the situation. For example, if both the incumbent and PCC share parishioner data, they'll likely be data controllers. The phrase "incumbent or priest-in-charge" may be used generically to include all ministers or specifically for those in that role, affecting who is a data controller for shared data. Providing personal data and privacy notice The parish must provide an individual with their personal data when first provided. If third-party data is provided, the privacy notice should be given within a reasonable time period, such as one month, initial communication, or disclosure to another recipient. The privacy notice should also be published on the website for future reference and linked to every page. Sensitivity is key when providing notices, especially in discussions like funeral arrangements. A brief summary can be included with a link to the full notice. Children are entitled to their own rights regarding data, starting from age 12. An age-appropriate privacy notice should be provided to children once they reach this age. A subject access request (SAR) is when an individual asks for copies of personal data held about them. Requests must be in writing and do not need to be labelled as such. Guidance on retention periods can be found online, but it's recommended to seek advice before destroying documents. Retention periods vary widely. For children's activities, records are kept for 50 years after the activity ceases. Safeguarding records are kept until they may be relevant to an inquiry or disclosure. Given article text here risk assessments should be stored securely, with access limited to 70 years after the last contact with an individual. Personnel files for employees or volunteers working with children or vulnerable adults can also be retained for up to 75 years. Application forms for unsuccessful applicants should be shredded and destroyed within a year of the role being filled. However, using online document storage systems like Google Drive or Dropbox may pose data protection concerns. To ensure compliance, it's essential to conduct a data protection impact assessment (DPIA) before storing personal data. This involves considering factors such as necessity and proportionality, risks, and mitigation strategies. Some key questions to ask when selecting an online document storage system include: * Is there a risk of documents being downloaded to an individual's personal computer? * Can access permissions be changed inadvertently? Using "off the shelf" systems may not be sufficient for sensitive information, such as safeguarding or child protection data. Consider purchasing software specifically designed to protect high-risk information. When using online storage, it's also essential to understand the role of a data processor and read relevant FAQs, including those provided by Data processors (#A). Following up with national church officers regarding weddings, baptisms, and funerals from past years, we're looking for clarification on certain procedures. It's suggested that anniversary cards can be sent to wedding couples without consent, as long as the recipient is someone you have regular contact with - which doesn't necessarily mean frequent contact. For instance, if someone only attends an Easter service every other year, they would still qualify as being in regular contact. These cards are a great way to stay in touch and could include a mention of the church's website or a friendly reminder to visit it. However, if you do decide to include any promotional content encouraging them to look at what the church is up to, this might be considered marketing, and consent would likely be needed. For email communications, things are a bit more restrictive. To avoid counting as marketing, it's generally necessary to get explicit consent from recipients before sending them anything related to church events or activities. This applies not only to promotional emails but also to any communication that includes encouraging language about the church. Regarding invites to the All Souls Service for past funerals, no consent is required if the person you're contacting has regular contact with the church. However, in cases where there's little to no prior connection - as might often be the case with family members of the deceased - it's best to ask verbally if they'd like to stay in touch and then follow up with a card or letter that includes a consent form for them to sign. It's worth noting that the GDPR primarily applies to living individuals, so records related to past funerals can generally be kept as they are. However, if you do choose to keep these records, it's essential to be transparent about why this is being done and how long the data will be stored. A clear explanation in your privacy notice or an accompanying information leaflet could help clarify this for families. Lastly, with regards to communication between schools and parents regarding church events outside of school life, there's a bit of confusion. While some might argue that seeking consent is not necessary, there's also a risk involved in taking a more relaxed approach. It seems the "belt and braces" approach - or being overly cautious - would be to seek consent each time. However, this could be seen as creating unnecessary hurdles for community outreach and engagement. The ICO recommends that schools notify parents and pupils about practices that may involve sharing personal data, even if consent isn't initially sought. This allows parents and older pupils to object, which should be recorded by the school. Any material intended for these individuals should not be sent home with them. The church material should be passed to the school for distribution. Schools must obtain consent before passing on personal data to the wider church or any other organisation. If a parent wants to attend a church event, they can either contact the relevant parish directly or give their consent to the school sharing the information. The DBE and DGAT will provide schools with direct guidance on implementing GDPR. The Diocese website's downloadable forms may be updated to allow individuals to opt out of sharing information with other bodies or organisations. Schools should obtain specific permission before sending named invitations to special services. The Church can discuss the Parish Giving scheme in person with parishioners, but they must have a conversation and provide fact sheets for those interested. Schools should send copies of personal details forms and confidential declaration forms to the Diocese for confidential shredding after a DBS check is completed. Personnel information should be recorded and kept according to data retention guidelines. Under GDPR, religious not-for-profit bodies may process special categories of personal data without consent if it's for legitimate purposes and relates only to members or former members. This exception applies to certain types of marketing communications. Parents cannot give consent on behalf of their children; instead, the child should exercise their own rights once they are mature enough (usually aged 12). eg, by requiring both the parent and the child to sign the consent form until the child is 16. For children who do not have sufficient maturity (ie, the majority of those aged 11 and younger) the parent can give consent on behalf of their child. If you are offering an online service to a child and you are relying on consent as the basis for doing this then the consent can come from the child once the child is aged 13. In other words, the general rule that children can exercise their rights from and including the age of 12 is displaced for online services where consent is sought. Regarding contacting family members who have provided personal details through various life events such as funerals, weddings, and baptisms, it's essential to consider their privacy notice. You should inform them that you have obtained their contact information and provide a copy of your privacy policy. However, the need for consent will depend on the purpose of the contact. For instance, if it's an invitation to a fundraising event, consent is usually necessary. In practice, "consent" means something must be freely given, specific, informed, and unambiguous. It doesn't necessarily have to be in writing, but it should be explicit as well. When considering GDPR requirements, keep the following points in mind: You should seek consent through a form where individuals can tick a box to give their consent (opt-in). Breaking down consent into smaller parts is also essential. You must not bundle consent with other matters and must inform individuals of their right to withdraw their consent. Additionally, you must keep records of obtained consents. Organisational measures for data protection include staff training, written policies and procedures, and audits to ensure compliance. Applying these principles in practice involves considering how to secure data in various situations, such as when working remotely or using family computers. Encryption is a method of encoding data so it cannot be accessed without the correct key or password. However, not all password-protected devices are encrypted. Using photographs from recent events in parish newsletters typically requires consent, especially for children under 12, who require parental consent until they reach that age, and then only from themselves at 16. Losing a laptop containing sensitive staff and payroll information without encryption necessitates informing the ICO within 72 hours unless the risk is low. Notifying data subjects, insurers, and possibly law enforcement may also be necessary due to potential identity theft. Cyber threats are a concern for parishes with inadequate protection measures in place, which can lead to GDPR breaches if personal data is at risk. Resources like Cyber Essentials, a government-backed scheme with cyber security standards, are available online. The upcoming consent requirement for marketing communications from May 2018 affects parish activities. While sending the Benefice Magazine, addressed to residents rather than specific individuals, may not require consent, it's essential to consider using contractors and handling personal data carefully, including IT matters. GDPR Right to Be Forgotten and Data Protection for Parish Matters at the very least we suggest they should be encrypted. Can we keep personal data for historical research purposes without consent? Yes, but with safeguards. Individuals have a right to object. Do we need consent before sharing info about volunteers who help out in the Parish? No, as long as it's only shared within the Parish community. If it's made public, consent is required. Can I use contact details from the electoral roll to send Church news and events? No, without consent. As a general rule, you can send info by post if transparent, within their expectations, and they're a member or former member of the Parish. However, for email communications, consent is usually needed. The CRR requires posting the electoral roll on the Church door before the Annual Parochial Council meeting. What are the implications vis-a-vis the Data Protection Act? You can publish it in this way as you're under a legal obligation. Just be transparent with individuals beforehand. If you want to publish elsewhere, consent is likely needed. Once people agree to be in a directory, it's hard to ensure their info won't be shared. As revised shall be published, along with a list of names removed from the roll since the last revision or formation, for at least 14 days before the annual parochial church meeting, typically displayed near the principal door of the parish church. This meets GDPR requirements as a legitimate activity for not-for-profit bodies, allowing data processing without consent for members, former members, and those with regular contact, provided no third-party disclosure occurs. The CRR, part of the Synodical Government Measure 1969, dictate relevant forms for administrative matters handled by the PCC. Forms state names will be published near the church door. The process already includes public notification on or near every church door in the parish and licensed buildings, giving individuals a chance to object before their name is entered on the electoral roll. If an individual objects but still applies, they implicitly consent to data processing. Providing additional information, such as display duration, can be done in a covering letter with enrolment forms. Those with sensitive positions should notify not to have details made public. Data sharing for deanery synod elections and churchwarden elections is allowed without consent, as stipulated in the CRR. The Rules state that results will be sent to the Diocesan Electoral Registration Officer, expecting candidates' data to be shared with the diocese. Children's Data Protection Under GDPR As a parish in a multi-parish benefice, it is essential to understand how GDPR applies to your situation. According to the ICO, if an organisation offers services over the internet directly to children under the age of 13, parental consent is required for processing their personal data lawfully. It's crucial to document consent for processing personal data under the GDPR, ensuring that it meets the required standards. If obtaining high-standard consent is challenging, an alternative legal basis or cessation of data processing might be necessary. Under the GDPR, consent must be verifiable and freely given, with clear affirmative action from individuals involved. Silence, pre-ticked boxes, or inactivity won't suffice for consent. Data subjects should also be informed of their right to withdraw consent at any time. Incumbents, as separate data controllers, are responsible for managing personal data according to the GDPR's guidelines, applicable to both incumbents and PCCs (Parochial Church Councils). Safeguarding advice emphasizes retaining records, such as parish magazines, which can be used as evidence. This raises questions about the right to erasure under the GDPR. The "right to be forgotten" allows data subjects to request erasure of personal data in specific situations, including when consent is withdrawn or the purposes for processing have ceased. However, statutory powers granted by the Inquiries Act 2005 may prevent destroying relevant personal data, such as that related to the IICSA (Independent Inquiry into Child Sexual Abuse). Moreover, publicly available material like parish magazines is exempt from the "right to be forgotten" since it's already in the public domain.