



GDPR NOTICE

The new General Data Protection Regulation (GDPR), significantly expands the data privacy and protection regime within the European Union (EU). St. Columba's Catholic Primary School, alongside its suppliers and contractors, must comply with these rules where applicable.

St. Columba's Catholic Primary School places high importance on information security and we have engaged in a companywide programme to address the requirements of GDPR and the use of data, specifically personal data. This involves working with our suppliers and partner organisations to ensure they can meet these obligations.

The key elements of our programme include:

- **GDPR Gap Analysis** – St. Columba's Catholic Primary School has engaged the DPO Centre Ltd., in providing Data Protection Officer (DPO) services and our DPO has conducted a GDPR Gap Analysis. St. Columba's Catholic Primary School has taken an agile approach in achieving the set targets. All required policies have been updated to GDPR standard and we continue to enhance our systems and processes in response.
- **Data Impact Assessments, Inventories and Mapping** – St. Columba's Catholic Primary School has conducted a Data Protection Impact Assessment (DPIA) across the organisation, which includes the preparation of a data asset register and identification of associated third party processors. As outlined under GDPR Articles 35 and 36, the DPIAs identify the relevant data components for ensuring adherence to the GDPR Principles. The DPIA describes the nature, scope, context, lawful basis and purposes of the processing; assesses necessity, proportionality and compliance measures; identifies and assesses risks to individuals; and identifies any additional measures to mitigate those risks. The data flow mapping identifies the method of collection, location, storage, sharing, security, retention and deletion of information across the complete data life cycle as applicable between St. Columba's Catholic Primary School, its data subjects and third-parties.
- **Policy Enhancement** – St. Columba's Catholic Primary School has updated its existing policies to GDPR standard and has created new policies where required. This includes refreshing our Privacy Policies and Data Breach Policy, Supplier and Third-Party agreements, with a specific GDPR focus. Following the ICO recommendations, [Organisation Name] is also adopting a new approach to Data Subject Access Requests for recording requests and sharing requested personal data. A new Data Protection Policy and a companywide Data Retention Policy has also been created.
- **Training and Culture** – St. Columba's Catholic Primary School's DPO has supported with GDPR awareness-raising and training of staff involved in processing operations, and the related audits as stated under Article 39(1)(b). St. Columba's Catholic Primary School has completed training and assessment for all staff on GDPR data handling procedures and requirements, specific to the role of the employee and companywide responsibility.

- **Third-party relationships** – Following our data mapping exercise, we have reviewed all third-party relationships that are in scope for compliance with GDPR Article 28, including all contractual agreements. We are working with these third parties to update agreements where needed, within the appropriate relationship terms; controllers, processors, suppliers and contractors.
- **Technology** – St. Columba’s Catholic Primary School continually reviews data and information security protection controls to maintain their efficiency and effectiveness, as outlined under Articles 25 and 32 of GDPR. St. Columba’s Catholic Primary School has implemented the ISO 27001 security controls.
- **Website Data Collection, Consent, and Privacy** – St. Columba’s Catholic Primary School website is updated to include a Privacy Policy and obligations to implement compliant disclosures and transparency notices when receiving personal information from data subjects.
- **Client Agreements (Business-to-Business)** – St. Columba’s Catholic Primary School continues to respond to all Client Agreements and addendums that address the GDPR requirements. Also, in order to meet the requirements of GDPR Article 28(3), [Organisation Name] has sent to all its clients a notification of all appointed sub-processors acting on its behalf, in order to meet the obligation to clients.