

'Shine like stars in the world'
Philippians 2:15



St Paul's CE Primary School

Article 30 Register of Processing Activities

[Our Vision](#)

Our school is one family, united in love and deeply rooted in our Christian values, where together on life's journey we flourish, striving for excellence in all that we do. Inspired by the transformation of St Paul, and enlightened by the glory of God, we will shine like stars to make the world a better place.

[Our Core Values](#)

Love, Forgiveness, Faith, Friendship, Hope and Peace.

ST PAUL'S CE PRIMARY SCHOOL
ARTICLE 30 – REGISTER OF PROCESSING ACTIVITIES

Article 30 Declaration – St Paul's CE Primary School

What is this document?

The UK General Data Protection Regulation (UK GDPR) requires that all data controllers and processors publish a record of processing (Article 30 Clause 1). This document provides this for our school.

- (a) The name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

The data controller is:

St Paul's CE Primary School
Ringwood Way
Winchmore Hill
London N21 2RA
Telephone: 020 8360 3137
Email: office@st-pauls.enfield.sch.uk

The Data Protection Officer may be contacted by email:

Schools.Data.Protection.Officer@enfield.gov.uk quoting our school name or by post:
Data Protection Officer – St Paul's CE Primary School
Enfield Council
Civic Offices
Silver Street
Enfield
EN1 3XA

- (b) the purposes of the processing;

Our processing covers the following purposes:

- enabling us to deliver education, including compliance with the wide range of statutory requirements on us as a school
- contact the right people about issues
- ensure a healthy, safe environment for learning
- carry out our functions as an employer

- (c) a description of the categories of data subjects and of the categories of personal data;

We keep data about the following classes of people:

- pupils of our school, including prospective pupils
- people that have responsibility for our pupils (such as parents, carers etc.)
- our staff and volunteers, the school's workforce

- (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

We disclose data to the following categories of recipients:

- The data subjects
- Parents of children in our school
- Schools workforce for the purposes of their work
- Our governing body
- The local authority (Enfield Council)
- The Department for Education

ST PAUL'S CE PRIMARY SCHOOL
ARTICLE 30 – REGISTER OF PROCESSING ACTIVITIES

- The local health boards
- Agencies involved in safeguarding
- Our service providers with whom we have contracts and appropriate Data Processing Agreements.

We may also make other disclosures as consented from time to time by parents.

- (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of appropriate safeguards;

Our data is held within the UK and countries with an adequacy decision from the UK regulator.

Our data is held both within the European Economic Area and the United States of America.

Some of our provision is provided by Microsoft, CPOMS using Microsoft and this is covered by EU Model Contractual Clauses.

A major part of our provision is provided by Google and this is covered by EU Model Contractual Clauses.

A major part of our provision is provided by J2E, using Amazon AWS, and this is covered by EU Model Contractual Clauses.

Our school management system is RM Integris, our school finance system is RM Finance and our mail and other systems are LGFL, Tapestry, e4education, Jigsaw, EdShed (data is stored in the UK and USA), Maths Circle, Kapow, Odizzi, Collins (EEA data storage) and our remote learning is J2E. Data resides in the UK for all of these.

- (f) where possible, the envisaged time limits for erasure of the different categories of data;

The time limits for our retention of data are documented in our Data Retention and Disposal Policy which is available on request. For most pupil data, this is as required by law being date of birth of pupil plus 25 years.

- (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

Article 32(1) measures are documented below:

- (a) *the pseudonymisation and encryption of personal data;*

We use encryption where possible for data on end user devices; encryption is always used where electronic data is in transit outside of our school. We do not use pseudonymisation within the school.

Electronic data access by parents and pupils outside the schools takes place on their own equipment; we encrypt in transit but it is not practicable to force encryption on these personal devices.

- (b) *the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*

Confidentiality – all systems have role based access control and many are also restricted to access only from our school network. There are policy and discipline frameworks in place to provide further controls, and access is logged.

Integrity – we regularly review data on our systems and they are subject to audit. There are also additional verification controls on some systems.

Availability / Resilience – there are service level agreements in place for cloud-based services. For on-site services we use methods such as replication of equipment (e.g. redundant power supplies, RAID) where necessary, and protection for power outages such as uninterruptable power supplies.

ST PAUL'S CE PRIMARY SCHOOL
ARTICLE 30 – REGISTER OF PROCESSING ACTIVITIES

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

For cloud services this is dependent on the cloud supplier; we have contractual controls regarding backup and restore as required in these contracts. For on-site services we have regular backups which include testing of backups to ensure recoverability.

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Audits are carried out on our systems; backup testing is undertaken. Where risk warrants, external tests such as penetration testing are used.

Reviewed by Denise Zmajkovic and Clare Cresswell	Autumn Term 2022		
Next Revision (Please highlight as appropriate) or in line with the update LA policies	Annual	Bi-annual	Tri- annual
To be reviewed	In line with the updated LA policies		