Article 30 guidance – Suffolks Primary School

What is this document?

The UK General Data Protection Regulation (UK GDPR 2021) requires that all data controllers and processors publish a Record of Processing, ROPA (Article 30This exists as an inventory of all data processing activities including the types of data that are processed by schools. The document outlines the following: -s

(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 Saira Patel - Suffolks Primary School

The Data Protection Officer may be contacted by email:

Schools.Data.Protection.Officer@enfield.gov.uk quoting our school's name

or by post:

Data Protection Officer - Suffolks 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
- 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.

No transfers are made to countries outside the United Kingdom.

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

Some of our provision is provided by Microsoft and this is covered by EU Data Boundary and IDTA (Internation Data Transfer Agreement).

(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 on our website. 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.

Minimum standard: Schools should use strong encryption where possible, for data on end user devices; encryption should always be used where electronic data is in transit outside of our school. School should also consider whether it is necessary to pseudonymise or anonymise data. The schools should implement a minimum level of TLS 1.3 and/or TLS 1.2, AES with 128 encryption.

Electronic data access by parents and pupils outside the schools takes place on their own equipment; we encrypt the data in transit (when sharing information via emails), but it is not possible e to enforce encryption on individuals personal devices; although they should also be bound by t standards (followed by the School regarding data security).

(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.

Minimum standard: Data quality checks (reviews of the accuracy of the data) should be conducted in line with consideration of the school's retention schedules.

Availability / Resilience – Schools should utilise manual and records management systems to store data. The data is arranged in a format and order that enables those with permitted access to locate them, when required.

Minimum standard:

Schools are required to ensure that personal data and the systems (manual and technological) used to store it, are safe, secure and accessible to those that authorised to access the records, when required.

Schools should have service level agreements (SLAs) in place for cloud-based services. Methods such as replication of equipment (e.g. redundant power supplies, RAID) should be implemented for on-site services where necessary, and protection for power outages such as uninterruptable power supplies.

(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.

Minimum standard: 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.

Minimum standard: Audits should be carried out on school systems; and backup testing should be undertaken. Where risk warrants, external tests such as penetration testing should be conducted periodically.