Article 30 Declaration – Forty Hill CE School

What is this document?

The General Data Protection Regulation 2016 (GDPR) as enacted in the UK by the Data Protection Act 2018 requires that all data controllers and processors publish a record of processing (GDPR 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 Forty Hill CE School

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 - <Forty Hill CE 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 European Economic Area.

Our data is held both 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 Model Contractual Clauses.

(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 "retention schedule, 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.

(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.