

# GDPR

We at IQRA Primary School are committed to ensuring the data we hold on Governors, Trustees, our families, students, staff and any of the third parties we work with is processed legally and protected.

We know that complete GDPR compliance can only be achieved through a collaborative and transparent approach and we also want to ensure that this is comprehensive and complete.

We have been working on the following:

- Identification of a Data Protection Officer
- Data mapping and Data Asset Register
- Embedding data privacy into all our processes
- Information security risk
- Third party risk and our data partners
- Preparing to respond to individual complaints and data subject access requests (DSARs)
- Data Privacy Breach procedures
- As well as ongoing monitoring

## GDPR Roll Out

We have started to roll out new GDPR privacy notices and we will be publishing a new GDPR/Data Protection Policy. We will ensure that all processing of data done in IQRA Primary School complies with GDPR

There are six lawful processing conditions:

- Compliance with a legal obligation
- Performance of a contract
- Legitimate interest
- Public interest
- Vital interest
- Consent

**Consent is changing** to be more explicit/transparent so at the point of data collection, the individual will need to be informed exactly how their data will be used and who it will be shared with.

## Governance Structure and Data Protection Officer

Data privacy will be discussed regularly at each Governing Body meeting and regularly reviewed by senior leaders within school.

IQRA Primary School's named Data Protection Officer (DPO) is Paul Clifford (GDPR consultant at Sapphire Consulting Group) and the DPO Link Governor is Maria Smith.

Maria will lead the teams in the school, helping embed data privacy into operations whilst also monitoring activity on an ongoing basis. Paul will oversee this work and act as an auditor and critical friend and assist where required. There will be regular training for all staff to ensure a deeper level of understanding, allowing them to identify any risks and stop them from happening.

### **Data Mapping and Data Asset Register**

We are completing our data mapping exercise and this document will be regularly revised and revisited. We are identifying what data we have, where it is held, how we access it, the classification of the data, records for transfer and flow charts to show how it moves between systems and processes.

A lot of information that already exists is held across several systems, so we are implementing a **Data Asset Register**, which will capture all data processing, aiding transparency and supporting the tight controls which are required to ensure compliance.

### **Embedding Data Privacy into day to day life of the school – Training and Awareness**

We are launching an internal initiative called IQRA compliant. This ongoing program has 4 key principles to ensure our team members do the right thing:

- We will ensure we know what we can do with data, and if unsure, we'll ask
- We will be clear about how we're going to use data
- We will ensure we protect the data we hold/process
- We will ensure compliance, both individually and as a team

Underpinning this is not only communication, but clear policies and procedures, plus mandatory training for all staff.

### **Information Security Risk**

We are implementing robust systems to manage our school network.

This will include technical security measures (e.g. intrusion, detection, firewalls, monitoring), encryption of personal data, restricted access to personal data, protection of our physical premises and hard assets, maintaining security measures for our staff, a data-loss prevention strategy and regular testing of our security systems.

### **Third Party Risk and our Data Partners**

Due diligence prior to working with a third party is key to ensure data has been gathered lawfully, and to ensure any data we share will be secure. If any third-party partners need to comply with GDPR, we'll ensure they do.

### **Responding to individual complaints and data subject access requests (DSARs)**

We already have a very robust process for dealing with consumer queries, this will now be expanded to include data subject access requests (DSAR). The key difference under GDPR is the timescale for response to a DSAR is reduced from 40 days to 30 days, which we do not foresee as an issue.

## **Data Privacy Breach Management Program**

We are implementing an effective data privacy incident and breach management plan, which we will continue to review and enhance as required.

There seems to be a lot of misconceptions about breach reporting, therefore we have really welcomed the ICO's blog on this topic.

Extract from the blog:

“Under the GDPR there is a requirement for organisations to report a personal data breach that affects people's rights and freedoms, without undue delay and, where feasible, not later than 72 hours after having become aware of it.

Organisations will have to provide certain details when reporting, but the GDPR says that where the organisation doesn't have all the details available, more can be provided later.

The ICO will not expect to receive comprehensive reports at the outset of the discovery or detection of an incident – but we will want to know the potential scope and the cause of the breach, mitigation actions you plan to take, and how you plan to address the problem.”

The GDPR does not provide an explicit time limit within which the processor must alert the controller, except that it must do so “without undue delay”. Therefore, WP29 recommends an immediate notification by the processor to the controller, with further information about the breach provided in phases as information becomes available. This is important to help the controller to meet the requirement of notification to the supervisory authority within 72 hours.

Our position is, the regulation states without “undue delay”, therefore this is what we will abide by. However, we recognise that the clock will only start ticking when we become aware there has been an incident.

## **Ongoing Monitoring**

Monitoring covers many areas at IQRA Primary School.

Internally we conduct audits and ad-hoc walk-throughs to make sure we are doing the right thing. A weekly regulatory monitoring report is issued to ensure we identify (and then action) privacy compliance requirements, such as changes in the law or best practice.

Paul Clifford

May 2018