



UK General Data Protection Regulation Policy (UK GDPR)

February 2021

Key Points

Markeaton Primary School collects and uses personal information (referred to in the General Data Protection Regulation as personal data) about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable the provision of education and other associated functions. In addition, the school may be required by law to collect, use and share certain information.

Markeaton Primary School is a registered Data Controller with the Information Commissioner's Office (ICO). Details are available on the ICO website.

Markeaton Primary School issues a Data Privacy Notice to all pupils/parents/staff. This summarises the information held on individuals, why it is held and the other organisations to whom it may be passed on.

Markeaton Primary School employs J. A. Walker, Solicitor, as our Data Protection Officer (DPO).

Purpose

This policy sets out how the school deals with personal information correctly and securely and in accordance with the UK GDPR, and other related legislation.

This policy applies to all personal information, however it is collected, used, recorded and stored and whether it is held on paper or electronically.

All school staff and governors involved with the collection, use, processing or disclosure of personal data will be trained appropriately, aware of their duties and responsibilities and will adhere to this policy.

What is Personal Information/Data?

Personal information or data is information which relates to a living individual who can be identified from that data, or from that data in addition to other information available to them. Personal data includes (but is not limited to) an individual's, name, address, phone number, date of birth, photograph, ethnicity, bank details and other information that identifies them.

Schools often collect sensitive data for DfE and LA requirements and of course pupil data may contain information about safeguarding, SEN or health needs. Information about other family members may also be on the school file.

Every school also has to publish a Privacy/Fair Processing Notice on their website.

Main principles of UK GDPR

The UK GDPR establishes six principles that must be adhered to at all times:

1. Lawfulness, transparency and fairness

School must have a legitimate reason to hold the data. We explain this in the Data Privacy Notices on the website. We often ask for consent to use data about a pupil for a particular purpose. If you wish to withdraw consent, we have a form to complete to allow us to process your request. There are some instances where you cannot withdraw consent as explained in 'Data Subjects' Rights'.

2. Collect data for a specific purpose and use for that purpose

Data cannot be used for a purpose that it was not originally collected for, or where notice has not been given about how data may be used after collection.

3. Limited collection

Markeaton Primary School should only collect the minimum amount of data needed for a particular task or reason. If there is a breach or a hack, only limited information can be lost.

4. Accuracy

Data collected should be accurate, and steps should be taken to check and confirm accuracy. We do this when pupils join the school and check on an annual basis. If a Data Subject feels that the information held is inaccurate, should no longer be held by the Controller or should not be held by the Controller in any event, a dispute resolution process and complaint process can be accessed, using the suitable forms.

5. Retention

Markeaton Primary School has a Records Management and Retention Policy that explains how long we store records for. This is available on request.

6. Security

Markeaton Primary School has processes in place to keep data safe. That might be paper files, electronic records or other information. See Records Management and Retention Policy.

Who is a 'data subject' ?

Someone whose details we keep on file. Some details are more sensitive than others. The UK GDPR sets out collection of details such as health conditions and ethnicity, which are more sensitive than names and phone numbers.

Data Subjects' rights

Data Subjects have a right:-

- to be informed
- of access to data stored about them or their children
- to rectification if there is an error on the data stored
- to erasure if there is no longer a need for school to keep the data
- to restrict processing, i.e. to limit what is done with their data
- to object to data being shared or collected

There are other rights that relate to automated decision making and data portability that are not directly relevant in schools.

Data subjects' rights are also subject to child protection and safeguarding concerns, sharing information for the prevention and detection of crime. Schools also have legal and contractual obligations to share information with organisations such as the Department for Education, Social Care, the Local Authority and HMRC amongst others. In some cases, these obligations override individual rights.

Subject Access Requests

You can ask for copies of information that we hold about you or a pupil (for whom you have parental responsibility). This Subject Access Request process is set out separately. You need to fill out the form, and you may need to provide identification evidence for us to process the request.

We have to provide the information within a month, but this can be extended if, for example, the school was closed for holidays. The maximum extension is up to two months.

When we receive a request we may ask you to be more specific about the information that you require. This is to refine any queries to make sure you access what you need, rather than sometimes getting a lot of information that may not be relevant to your query.

In some cases we cannot share all information we hold on file if there are contractual, legal or regulatory reasons.

We cannot release information provided by a third party without their consent, or in some cases you may be better to approach them directly, e.g. school nurses who are employed by the NHS.

We will supply the information in an electronic form.

If you wish to complain about the process, please see our complaints policy and later information in this DPA policy.

Who is a 'data controller'?

Our school governing body is the data controller. They have ultimate responsibility for how school manages data. They delegate this to data processors to act on their behalf.

Who is a 'data processor'?

This is a person or organisation that uses, collects, accesses or amends the data that the controller has collected or authorised to be collected. It can be a member of staff, a third-party company, possibly a

governor, a contractor or temporary employee. It can also be another organisation such as the police or the LA.

Data controllers must make sure that data processors are as careful about the data as the controller themselves. The GDPR places additional obligations on organisations to make sure that Data Controllers require contractual agreements to ensure that this is the case.

Processing data

School must have a reason to process the data about an individual. Our privacy notices set out how we use data. The GDPR has 6 conditions for lawful processing and any time we process data relating to an individual it is within one of those conditions.

If there is a data breach we have a separate policy and procedure to follow to take immediate action to remedy the situation as quickly as possible.

The legal basis and authority for collecting and processing data in school are:-

- consent obtained from the data subject or their parent
- performance of a contract where the data subject is a party
- compliance with a legal obligation
- to protect the vital interests of the data subject or other associated person
- to carry out the processing that is in the public interest and/or official authority
- it is necessary for the legitimate interests of the data controller or third party
- in accordance with national law.

In addition, any special categories of personal data are processed on the grounds of

- explicit consent from the data subject or about their child
- necessary to comply with employment rights or obligations
- protection of the vital interests of the data subject or associated person
- being necessary to comply with the legitimate activities of the school
- existing personal data that has been made public by the data subject and is no longer confidential
- bringing or defending legal claims
- safeguarding
- national laws in terms of processing genetic, biometric or health data.

Processing data is recorded within the school systems.

Data Sharing

Data sharing is done within the limits set by the GDPR. Guidance from the Department for Education, health, the police, local authorities and other specialist organisations may be used to determine whether data is shared.

The basis for sharing or not sharing data is recorded in school.

Breaches & Non Compliance

If there is non compliance with the policy or processes, or there is a DPA breach as described within the GDPR and DPA 2018 then the guidance set out in the Breach & Non Compliance Procedure and Process needs to be followed.

Protecting data and maintaining data subjects rights is the purpose of this policy and associated procedures.

See separate Breach & Non Compliance Procedures and Policy.

Consent

As a school we will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required.

However, in most cases data will only be processed if explicit consent has been obtained.

Consent is defined by the GDPR as “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”.

We may seek consent from young people also, and this will be dependent on the child and the reason for processing.

Consent and Renewal

On the school website we have ‘Privacy Notices’ that explain how data is collected and used. It is important to read those notices as it explains how data is used in detail.

Obtaining clear consent and ensuring that the consent remains in place is important for school. We also want to ensure the accuracy of that information.

For Pupils and Parents/Carers

On arrival at school you will be asked to complete a form giving next of kin details, emergency contact and other essential information. We will also ask you to give consent to use the information for other in school purposes, as set out on the data collection/consent form.

We review the contact and consent form on an annual basis. It is important to inform school if details or your decision about consent changes. A form is available.

Pupil Consent Procedure

Where processing relates to a child under 16 years old, school will obtain the consent from a person who has parental responsibility for the child.

Pupils may be asked to give consent or to be consulted about how their data is obtained, shared and used in certain situations.

Withdrawal of Consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent the school will consider each situation on the merits and within the principles of GDPR and also child welfare, protection and safeguarding principles.

Please complete the appropriate form.

CCTV Policy

Please see the CCTV Policy.

We use CCTV and store images for a period of time in line with the policy. CCTV may be used for:

Detection and prevention of crime

School staff disciplinary procedures

Pupil behaviour and exclusion management processes

To assist the school in complying with legal and regulatory obligations

Data Protection Officer

We have a Data Protection Officer whose role is to:-

- to inform and advise the controller or the processor and the employees who carry out processing of their obligations under the UK GDPR
- to monitor compliance with the UKGDPR and DPA
- to provide advice where requested about the data protection impact assessment and monitor its performance
- To be the point of contact for Data Subjects if there are concerns about data protection
- to cooperate with the supervisory authority and manage the breach procedure
- to advise about training and CPD for the GDPR

Our DPO is John Walker, Solicitor. info@jawalker.co.uk

Physical Security

In school, every secure area has individuals who are responsible for ensuring that the space is securely maintained and controlled if unoccupied, i.e. locked. Offices and cupboards that contain personal data should be secured if the processor is not present.

The Headteacher is responsible for authorising access to secure areas along with the Site Manager.

All Staff, contractors and third parties who have control over lockable areas must take due care to prevent data breaches.

Secure Disposal

When disposal of items is necessary, a suitable process must be used. This is to secure the data, to provide a process that does not enable data to be shared in error, by malicious or criminal intent.

These processes, when undertaken by a third party, are subject to contractual conditions to ensure UK GDPR and DPA compliance.

Hardware is disposed of/ recycled by the IT Technician.

Hard copy files are destroyed by the office.

Servers and Hard drives are cleansed by the IT Technician.

Portable and removable storage are destroyed / cleaned/ recycled by the office or IT Technician.

Complaints & the Information Commissioner Office (ICO)

The school Complaints Policy deals with complaints about Data protection issues.

There is a right to complain if you feel that data has been shared without consent or lawful authority.

You can complain if you have asked to us to erase, rectify, not process data and we have not agreed to your request.

We will always try to resolve issues on an informal basis, and then through our formal complaints procedure. Please complete the form, and we will contact you with more details about the timescale and process.

In the UK, it is the ICO who has responsibility for safeguarding and enforcing the DPA obligations.

Email: casework@ico.org.uk Helpline: 0303 123 1113 web: www.ico.org.uk

Review

A review of the effectiveness of UK GDPR compliance and processes will be conducted by the Data Protection Officer every 12/24 months.

February 2021

Review date May 2022

Approved at Governors' Meeting on 22.4.21.

Signed:

..... **for Governors**

..... **Headteacher**