Data Protection Policy

Contents

1 Overview

2 Scope and Applicability

3 General Policy

3.1 Objectives

3.2 ICO Registration

3.3 Introduction to the UK GDPR

3.4 Data Protection Principles

3.5 External Data Transfers

3.6 Safeguards

3.7 Data subjects' rights

3.8 Complaints

3.9 Consent

3.10 Security of data

3.11 Rights of access to data

3.12 Retention and disposal of data

3.13 Security Incidents

4 Roles and Responsibilities

5 Compliance

6 Risk Management

7 References

8 Definitions

9 Review

1. Overview

The purpose of this policy is to ensure that the school is committed to compliance with all relevant data protection laws in respect of personal data and to protecting the "rights and freedoms" of individuals whose information is collected. To that end, the school has developed, implemented, maintains and continuously improves data protection policies and procedures.

Moulton Chapel Primary School is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and the Data Protection Act (DPA).

2 Scope and Applicability

The school is a data controller and a data processor under the UK General Data Protection Regulation (UK GDPR). The UK regulator for Data Privacy is the Information Commissioner's Office (ICO).
https://ico.org.uk/for-organisations/guide-to-data-protection/data-protectionprinciples/
This policy applies to all School staff including temporary staff and contractors. Compliance with data protection legislation is the responsibility of all members of the school who process personal information. Therefore, this procedure applies to all personal data processed by the school.

3 General Policy

3.1 Objectives

The school is committed to complying with data protection legislation and good practice including:

- *Processing personal information only where this is strictly necessary for legitimate purposes*
- *Collecting only the minimum personal information required for these purposes and not processing excessive personal information*
- *Providing clear information to individuals about how their personal information will be used and by whom*
- *Only processing relevant and adequate personal information*
- *Processing personal information fairly and lawfully*
- *Maintaining an inventory of the categories of personal information processed by the school*
- *Keeping personal information accurate and, where necessary, up to date*
- *Retaining personal information only for as long as is necessary for legal or regulatory reasons or, for legitimate purposes*
- *Respecting individuals' rights in relation to their personal information, including their right of subject access*
- *Keeping all personal information secure*
- *Only transferring personal information outside the United Kingdom in circumstances where it can be adequately protected*
- *The application of the various exemptions allowable by data protection legislation*

3.2 ICO Registration

The school has notified the ICO that it is a data controller and that it processes certain information about data subjects. The school has identified all the personal data that it processes, and this is contained in the Information Asset Register (IAR).

A copy of the ICO Registration is retained by the school senior administrator and is available to view on the ICO website.

The ICO registration is renewed annually.

The school's nominated person is responsible, each year, for reviewing the details of registration, in the light of any changes to the school's size or structure.

3.3 Introduction to the UK GDPR

The Data Protection Act 2018 is a United Kingdom Act of Parliament which updates data protection laws in the UK and supersedes the Data Protection Act 1998. It is a national law which sits alongside the UK GDPR which from 1st January 2021 replaces the European Union's General Data Protection Regulation due to the UK's exit from the European Union.
The purpose of the UK GDPR is to protect the "rights and freedoms" of living individuals, to ensure that personal data is not processed without their knowledge and that it is processed lawfully.

3.4 Data Protection Principles

All processing of personal data must be done in accordance with the following data protection principles of the UK GDPR. The school's policies and procedures are designed to ensure compliance with them.

Personal data must be processed lawfully, fairly and transparently.

The UK GDPR stipulates the requirement for transparency whereby the controller has transparent and easily accessible policies relating to the processing of personal data and the exercise of individuals' "rights and freedoms".
Information must be communicated to the data subject in an intelligible form using clear and plain language commonly in the form of a privacy notice.

The specific information that must be provided to the data subject must as a minimum include:

- *The contact details of the school*
- *The contact details of the DPO*
- *The purposes of the processing for which the personal data are intended as well as the legal basis for the processing*
- *Who the personal data will be shared with*
- *The period for which the personal data will be stored*
- *The existence of the data subject rights*
- *The categories of personal data concerned*
- *Is the data transferred out of the UK*

- *Any further information necessary to guarantee fair processing*

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities, for example local authorities, Ofsted, or the Department of Health.
These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.
The intention to share data relating to individuals to an organisation outside of our school shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.
Any proposed change to the processing of an individual's data shall first be notified to them.

Under no circumstances will the school disclose information or data:

- *that would cause serious harm to the child or anyone else's physical or mental health or condition*
- *indicating that the child is or has been subject to child abuse or may be at risk of it,*
- *where the disclosure would not be in the best interests of the child*
- *recorded by the pupil in an examination.*
- *that would allow another person to be identified or identifies another person as the source, unless the person is an employee of the school or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent.*

The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed in the form of a reference given to another school or any other place of education and training, the child's potential employer, or any national body concerned with student admissions
Transparency | ICO

Personal data can only be collected for specified, explicit and legitimate purposes

- *Data obtained for specified purposes must not be used for a purpose that differs from those documented in the Information Asset Register (IAR) and stipulated in the Privacy Notice.*

Personal data must be adequate, relevant and limited to what is necessary for processing

- *The school is responsible for ensuring that information, which is not strictly necessary for the purpose for which it is obtained, is not collected.*
- *All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be approved by the school.*
- *The school will review data collection methods on a regular basis to ensure that collected data continues to be adequate, relevant and not excessive.*
- *If data is given or obtained that is excessive or not specifically required by the school's documented procedures, the school's nominated contact is responsible for ensuring that it is securely deleted or destroyed in line with the school's retention schedule.*

Personal data must be accurate and kept up to date

- *Personal Data that is processed must be reviewed and updated as necessary. No data should be retained unless it is reasonable to assume that it is accurate.*
- *The Head Teacher is responsible for ensuring that all staff members are trained in the importance of collecting accurate data and maintaining it.*
- *It is also the responsibility of individuals to ensure that data held by the school is accurate and up to date. Completion of an appropriate registration or application form etc. will be taken as an indication that the data contained therein is accurate at the date of submission.*
- *Data subjects should notify the school of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the school to ensure that any notification regarding change of circumstances is noted and acted upon within 1 month.*
- *The school is responsible for ensuring that appropriate additional steps are taken to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.*
- *The school's nominated contact will review all the personal data maintained by the school on a regular basis, by reference to the IAR, and will identify any data that is no longer required in the context of the registered purpose and will arrange to have that data securely deleted/destroyed in line with School's data retention schedule.*
- *The school's nominated contact is responsible for making appropriate arrangements that, where third party organisations may have been passed inaccurate or out-of-date personal information, for information about them that the information is inaccurate and/or out-of-date is not to be used to inform decisions about the individuals concerned and for passing any correction to the personal information to the third party required.*

Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

Personal and Sensitive Data:

All data within the school's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

The definitions of personal and sensitive data shall be as those published by the ICO for guidance:

https://ico.org.uk/for-organisations/guide-to-data-protection/keydefinitions/

The principles of the Data Protection Act shall be applied to all data processed:

- *ensure that data is fairly and lawfully processed*
- *process data only for limited purposes*
- *ensure that all data processed is adequate, relevant and not excessive*
- *ensure that data processed is accurate*
- *not keep data longer than is necessary*

- *process the data in accordance with the data subject's rights*
- *ensure that data is secure*
- *ensure that data is not transferred to other countries without adequate protection.*

Risk and impact assessments shall be conducted in accordance with guidance given by the ICO:
https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2014/02/privacyimpact-assessments-code-published/

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.
The security arrangements of any organisation with which data is shared shall also be considered and where required these organisations shall provide evidence of the competence in the security of shared data

- *Where personal data is retained beyond the processing date, it will be held securely in order to protect the identity of the data subject in the event of a data breach.*
- *Personal data will be retained in line with the School's Records Retention Schedule and, once its retention date is passed, it must be securely destroyed as set out in this procedure.*

Personal data must be processed in a manner that ensures its security.

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed. Data held by the school is secure, controlled and managed. The school's systems and network are regularly independently tested.

Security controls may be subject to audit and review by independent auditors.

The controller shall be responsible for and be able to demonstrate compliance with accountability.

The UK GDPR introduces the principle of accountability which states that the controller is not only responsible for ensuring compliance but for demonstrating that each processing operation complies with the requirements of the UK GDPR.

Specifically, controllers are required to maintain necessary documentation of all processing operations, implement appropriate security measures, perform DPIAs, comply with requirements for prior notifications, or approval from the ICO and appoint a DPO.

3.5 External Data Transfers

Personal data shall not be transferred to a country or territory outside the United Kingdom unless that country or territory ensures an adequate level of protection for the 'rights and freedoms' of data subjects in relation to the processing of personal data.

The transfer of personal data outside of the United Kingdom is prohibited unless one or more of the specified safeguards or exceptions apply.

3.6 Safeguards

An assessment of the adequacy by the data controller taking into account the following factors:

- *The nature of the information being transferred*
- *The country or territory of the origin, and final destination, of the information*
- *How the information will be used and for how long*
- *The laws and practices of the country of the transferee, including relevant codes of practice and international obligations*
- *The security measures that are to be taken as regards the data in the overseas location*

3.7 Data subjects' rights

Data subjects have the following rights regarding personal data that is recorded about them:

- *The right to be informed*
- *The right of access*
- *The right to rectification*
- *The right to erasure*
- *The right to restrict processing*
- *The right to data portability*
- *The right to object*

3.8 Complaints

Data Subjects who wish to complain to the school about how their personal information has been processed may lodge their complaint with the school.

If Data Subjects are not satisfied with the outcome of their complaint or the way in which it has been handled, they may also complain directly to the ICO.

3.9 Consent

The school understands 'consent' to mean that it has been explicitly and freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement, or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The consent of the data subject can be withdrawn at any time. The school understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them.

Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be active communication between the parties which demonstrate active consent. Consent cannot be inferred from non-response to a communication. For special category data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

In most instances consent to process personal and special category data is obtained routinely by the school using standard consent documents e.g. when a new member of staff signs a contract of employment, or during induction for participants on programmes.

Where the School provides online services to children, parental, or custodial authorisation must be obtained. This requirement applies to children under the age of 13.

3.10 Security of data

All Staff are responsible for ensuring that any personal data which the school holds and for which they are responsible, is kept securely and is not under any condition disclosed to any third party unless that third party has been specifically authorised by the school to receive that information and has entered into a confidentiality agreement.

Any third parties working with or for the school, and who have or may have access to personal information, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by the school without having first entered into an agreement which imposes on the third-party obligations no less onerous than those to which the school is committed, and which gives the school the right to audit compliance with the agreement.

All personal data should be accessible only to those who need to use it. The school will form a judgement based upon the sensitivity and value of the information in question, but personal data must be kept:

- *In a locked room with controlled access*
- *In a locked drawer or filing cabinet*
- *If computerised, password protected*
- *Encrypted if stored on mobile/removable devices*

Care must be taken to ensure that PC screens and terminals are not visible except to authorised members of staff of the school.

Manual records are not to be left where they can be accessed by unauthorised personnel and may not be removed from School premises without explicit authorisation.

Personal data will only be deleted or disposed of in line with the School's Retention Policy. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Storage drives of redundant PCs and mobile devices are to be removed and immediately securely destroyed.

Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site and appropriate security controls implemented.

Security controls may include:

- *Data encryption*
- *Password or PIN protected data*

- *Secure storage device*
- *Secure remote access to the data*
- *Not working in an environment that is not secure or safe such as an internet cafe*
- *Not keeping laptops or paper records overnight in a vehicle*

Other schools

If a pupil transfers from Moulton Chapel Primary School to another school, their records and other data that relates to their health and welfare will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.

Examination authorities

This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

Health authorities

As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

Police and courts

If a situation arises where a criminal investigation is being carried out, we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

Social workers and support agencies

In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

Educational division

Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

Right to be Forgotten:

Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped, and all their personal data is erased by the school including any data held by contracted processors.

Photographs and Video:

Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in school only.
Unless prior consent from parents/pupils/staff has been given, the school shall not utilise such images for publication or communication to external sources.
It is the school's policy that external parties (including parents) may not capture images of staff or pupils during such activities without prior consent.

Location of information and data:

Hard copy data, records, and personal information are stored out of sight and in a locked cupboard. This will be stored with the SENDCo. The only exception to this is medical information that may require immediate access during the school day.
Sensitive or personal information and data should not be removed from the school site; however, the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings or are on school visits with pupils.

3.11 Rights of access to data

Data subjects have the right to access any personal data (i.e. data about them) which is held by the school in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by the school, and information obtained from third parties about that person. SARs are dealt with as described in the SAR Procedure.

Disclosure of data

The school must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of the school's business.

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the DPO. The regulations allow for some exemptions. These too should be discussed with the DPO.

3.12 Retention and disposal of data

Personal data may not be retained for longer than it is required. Once a member of staff has left the school, it may not be necessary to retain all the information held on them. Some data will be kept for longer periods than others.

Disposal of records

The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.
All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.
All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process. Disposal of IT assets holding data shall be in compliance with ICO guidance:

https://ico.org.uk/media/fororganisations/documents/1570/it_asset_disposal_for_organisations.pdf

The school has identified a qualified source for disposal of IT assets and collections.
The school has also used a company to dispose of large amounts of sensitive data that is no longer required and also has internal shredding machines to support the day-to-day security.

Personal data must be disposed of in a way that protects the "rights and freedoms" of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion).

3.13 Security Incidents

The school is required to have internal breach reporting procedures in place as well as external breach reporting procedures.

All security incidents are recorded by the school and all staff have been trained to recognise both a security incident and a personal data breach.

The school notifies the DPO (ArkICT) of all incidents as soon as practical after the incident has been discovered.

When a personal data breach has occurred, the school in conjunction with the DPO will establish the likelihood and severity of the resulting risk to individual's rights and freedoms. If there is likely that there will be a risk, the ICO must be notified. The DPO will report serious data breaches within 72 hours of the incident to the ICO.

The UK GDPR states "A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

Any serious breach of data protection legislation will be dealt with under the school's disciplinary policy and may also be a criminal offence, in which case the matter will be reported to the ICO or Police.

4. Roles and Responsibilities

- *The Head Teacher and all those throughout the school are responsible for developing and encouraging good information handling practices.*
- *The Data Protection Officer (DPO), a role specified in the UK GDPR, is accountable for ensuring that compliance with data protection legislation and good practice can be demonstrated.*

  This accountability includes:

  1. *Development and implementation of the UK GDPR as required by this policy; and*
  2. *Security and risk management in relation to compliance with the policy.*
- *The school's nominated person has been appointed to take responsibility for the school's compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that the school complies with the UK GDPR, as do staff in respect of data processing that takes place within their area of responsibility.*
- *The school's nominated person has specific responsibilities in respect of procedures such as the Subject Access Request (SAR) Procedure and is the first point of call for staff seeking clarification on any aspect of data protection compliance before contacting the Head Teacher.*
- All individuals whose data is held by us, has a legal right to request access to such data or information about what is held. We shall respond to such requests within one month and the request should be made in writing to the Head Teacher

- *No charge will be applied to process the request.*
- *Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child.*
- *The school`s nominated person will be the conduit between the school and the DPO for security incident reporting.*
- *The school will ensure appropriate data protection training is provided for all staff.*
- *Staff are responsible for ensuring that any personal data supplied by them, and that is about them, to the school is accurate and up to date.*

5.0 Compliance

Compliance is mandatory and will be enforced for all employees, vendors and contractors. Non-compliance with this and other policies may be subject to disciplinary action, up to and including dismissal.

6.0 Risk Management

Risk management for the school is set out in the Risk Register.

7.0 References

None

8.0 Definitions

SAR- Subject Access Request
UK GDPR- The UK General Data Protection regulation
ICO- Information Commissioner's Office

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data, where the purposes and means of such processing is determined by UK law, the controller or the specific criteria for its nomination may be provided for by UK law. The school is a data controller.

Data Subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use,

disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent- means 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.

Child – The UK GDPR does not define the age at which a person is considered to be a child. The processing of personal data of a child under 13 years of age in relation to online services is only lawful if parental or guardian consent has been obtained.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

9.0 Review

This policy will be reviewed and updated on a regular basis, not to exceed 24 months.
Next review: Spring 2027