Horton Mill Community Primary School

Data Protection Policy

September 2019

Approved by Governors:

Date ……

Signed ……

1. Objectives

1.1. We recognise the need for legal compliance and accountability and endorse the importance of the integrity, availability, confidentiality, resilience and security arrangements to safeguard personal data. We also recognise that there are times that personal data is shared with, and/or received from, other organisations and that this needs to be in accordance with the law.

1.2. This policy sets out the key data protection obligations and accountability to which we are fully committed.

2. Scope

2.1. In order to fulfil our statutory and operational obligations we have to collect, use, receive and share personal, special personal and crime data about living people, eg,

- Pupils and their families
- current, past, prospective employees
- clients and customers
- contractors and suppliers
- Governors

2.2. This policy covers all aspects of handling personal data, regardless of age, format, systems and processes purchased, developed and managed by/or on behalf of us and any person directly employed or otherwise by us.

2.3. This policy meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

2.4. This policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

2.5. This policy reflects the commitment to data protection compliance to both UK and EU legislation, in particular the Data Protection Act 2018, the EU General Data Protection Regulation 2016 (GDPR).

3. Policy

3.1. Data Protection Officer (DPO): We will appoint a data protection officer who will be the key contact for the provision of independent advice on all things data protection. The DPO will provide advice and support when dealing data subject enquiries and communications with the Information Commissioners Office.

Data Protection Officer

Barbara Mulvihill
Data Protection Officer on behalf of Horton Mill Community Primary School:

West Street
Oldham
OL1 1UT

Email: DPO@oldham.gov.uk
Tel: 0161 770 1311

3.2. Definitions of personal data:

Personal data means 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;

In summary, anything and everything that can relate to a living person.

Special Personal data means 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

In summary, these are the data categories that are subject to additional controls in order to prevent unauthorised collection, use, access etc.

Crime data means criminal offence data, eg, alleged commission of offences or proceedings for an offence, (actual or alleged), including sentencing, other than it is USED for law enforcement purposes by competent authorities under part 3 of the Data Protection Act 2018 for the purposes of the prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security

In summary this type of personal data is subject to specific conditions and controls and a school is not a competent authority in relation to this.

3.3. Data Protection Principles: There are six principles which provide the framework for personal data handling and we as the data controller are accountable for compliance.

Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner

To be lawful an appropriate condition of processing needs to be identified. To be fair and transparent a privacy notices needs to be provided/available to the data subject whose personal data is being handled (data subject) and the law specifies what information must be communicated.

(b) processed for an explicit and specific purpose and not processed for other incompatible purposes. Scientific/historical/statistical research is not incompatible and nor is archiving in the public interest

Personal data should only be used for the stated lawful purposes, except where the law permits.

(c) adequate, relevant and limited to what is necessary for the purpose

Ensure that personal data is specific to the stated lawful purpose it is required for, is not excessive or unnecessary.

(d) accurate and, where necessary, kept up to date; ensuring that personal data that are inaccurate, are erased or rectified without delay

Ensure that personal data is correct and that any errors are rectified and where appropriate notified to recipients of the personal data

(e) personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed, but can be kept for longer if solely for scientific/historical/statistical research and archiving in the public interest purposes and is kept securely

Personal data should not be kept longer than necessary taking into account legal and operational requirements

(f) protection of the personal data using appropriate technical or organisational measures

These measures should be selected on the basis of identified threats and risks to personal data and the potential impact on the data subjects, we and any third parties who are sources, recipients, or processors of the personal data.

3.4. Mandatory obligations: we will ensure that we are appropriately registered with the Information Commissioner's Office (ICO) and create and maintain the mandatory Record of Processing Activities (ROPA), to be made available to the (ICO) upon demand

3.5. Data Privacy Impact Assessments (DPIA): are an important vehicle in ensuring that Data Protection by Design and by Default is part of business as normal. This ensure that privacy risks are considered within NEW technical systems and NEW day to day business operations. These privacy risk assessments must take place where there is a high risk to the privacy rights and freedoms of a data subject. Examples where these are likely to be required, include, but are not limited to, new systems and processes, new or different uses of personal data. Where a high risk is identified the DPO must be consulted before any new or changed processing is introduced to ensure adequate risk mitigation measures are implemented. Where risks are high and not adequately mitigated, a referral to the ICO must be made.

3.6. Data Collection, use and disclosure: We handle personal data that has been either collected from the data subject and/or other parties, eg, other people, public sector and regulatory organisations, private and voluntary sector organisations etc.

3.6.1. **Lawfulness**: We commit to the following:

- To only handle personal data where there is a legal basis to do so.
- Not necessarily rely on consent where there is an alternative lawful basis for processed. However, where consent/explicit consent, is the lawful basis, then we acknowledge that for consent to valid it must be freely given and capable of being withdrawn. Where consent cannot be obtained directly from the data subject then measures will be put in place to seek consent from an appropriate person, eg, parent, guardian, lawful representative etc. We will not send marketing material without obtaining consent
- If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).
- We will obtain written consent from parents/carers for photographs/videos of children to be used for communication/publicity/marketing materials.
- To provide data subjects with privacy notices that explain why the personal data is required and how the exercise their personal data rights.
- When handling special, and/or crime personal data, to conform to the required lawful conditions, specific policy requirements and inclusion in the ROPA
- In the event of a data subject exercising their personal data rights, we will assess the request and respond within the statutory timeline and provide a complaints process

3.6.2. Controls: We commit to the following:

- In the event of a personal data security breach, resulting in a high risk to the data subject(s), to notify the data subjects and/or the ICO as appropriate.
- Personal data will be subject to appropriate retention and security controls taking into account the nature of the data and the information risks. Personal data may be stored for longer periods where it is for archiving in the public interest, historical or scientific research purposes, or when determined by legislation or regulatory activity.
- When sharing and disclosing personal data this will be undertaken within the parameters of the law to prevent unauthorised access to personal data. A record will be kept and where appropriate formalisation of the arrangements will take place. Where appropriate DPIA's will be undertaken in advance of the sharing/disclosure.
- Ensure that in the processing of personal data within our supply chains includes contractual clauses required by law and that processing is only undertaken in accordance with our instructions at data controller.
- Not to transfer personal data outside of the European Economic Area (EAA) to countries with lower data protection standards unless appropriate safeguards apply, These controls include: a decision by the EU that the country has 'adequate' data protection legislation; that a company within the US is a signatory

to the EU/US Privacy Shield binding corporate rules or model contracts clauses are in place, or the law provides for this in defined circumstances

- To provide all staff and governors with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.
- To co-operate and provide information to the ICO and other regulatory bodies in pursuance of any investigation or enforcement action.

3.7. Offences: The data protection legislation contains specific offences:

3.7.1. It is an offence for a person knowingly or recklessly, without the consent of the data controller, to

- obtain or disclose personal data
- procure the disclosure of personal data to another person
- retain it without the consent of the original data controller.
- offer to sell, sell or buy the personal data obtained

.

3.7.2. It is an offence for a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller, or to knowingly or recklessly handle such data.

3.7.3. It is an offence to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the data subject making the request for access or portability would have been entitled to receive.

3.7.4. Enforced data subject access is an offence, ie, to require an individual to provide health and/or conviction /caution data by making a data subject access request in order to obtain their own personal data. This is relation to information required for the purpose of recruitment, continued employment or in connection with provision of goods and services to the public.

3.7.5. It is an offence to intentionally obstruct, or give false information to the ICO in the exercise of its powers under information notices and/or warrants.

4. Assessment and Monitoring

4.1. An assessment of compliance with requirements will be undertaken in order to provide:

- Assurance
- Gap analysis of policy and practice
- Examples of best practice
- Improvement and training plans

5. Responsibilities and Approvals

5.1. Governing Body:

The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2. Headteacher:

The Headteacher acts as the representative of the data controller on a day-to-day basis and is responsible for the approval of this policy.

5.3. Data Protection Officer:

The Data Protection Officer will be the key contact for the provision of independent advice on all things data protection. The DPO will provide advice and support when dealing data subject enquiries and communications with the Information Commissioners Office.

5.4. Governors/Employees:

All Governors and staff, whether permanent, temporary or contracted, including students, contractors and volunteers are responsible for ensuring they are aware of the data protection legislation requirements and for ensuring they comply with these on a day to day basis. Where necessary advice, assistance and training should be sought. Any breach of this policy could result in disciplinary action or could constitute a criminal offence.