Moorside
Primary School

DATA PROTECTION AND SECURITY POLICY
2019
This policy should be read in conjunction with:
Privacy Notices, Freedom of Information Guide and Social Media advice

Introduction
The school holds and processes information about employees, pupils and other data subjects for educational and other purposes, as detailed under the following headings in our Registry Entry with the Information Commissioner's Office:

- Education
- Educational Support and Ancillary Purposes
- School Administration
- Staff, Agent and Contractor Administration
- Advertising, Marketing, Public Relations, General Advice Services
- Crime Prevention and Prosecution of Offenders

Information is an integral part of the Data Protection Act 1998 and the School must take all reasonable steps to ensure that any personal or sensitive information held is stored securely. The Governing Body of the school has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions. In May 2018 the GDPR (General Data Protection Regulations) come into force and the school is required to appoint a DPO (Data Protection Officer) to ensure that practices are in place.

The Head Teacher and Governors of Moorside Primary School comply fully with the requirements and principles of the Data Protection Act 1984, the Data Protection Act 1988 and the GDPR. All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines. In summary the guidelines state that personal data will:

- Be processed fairly and lawfully
- Be obtained for a specified and lawful purpose and will not be processed in any manner incompatible with the purpose
- Be adequate, relevant and not excessive for the purpose
- Be accurate and up-to-date
- Not be kept for longer than necessary for the purpose
- Be processed in accordance with the data subject's rights
- Be kept safe from unauthorised processing and accidental loss, damage or destruction
- Not be transferred to a country outside the EC, unless that country has equivalent levels of protection for personal data, except in specified circumstances

Fair Obtaining and Processing
The school will notify all pupils (parents/carers), staff and other relevant data subjects of the types of data held and processed by the school concerning them, and the reasons for which it is processed by issuing Privacy Notices.

Definitions: "staff", "pupils" and "other data subjects" may include past, present and potential members of these groups. "Other data subjects" and "third parties" may include contractors, suppliers, contacts, referees, friends, family members, volunteers, placement students. "Processing" refers to any action involving personal information, including obtaining, viewing, copying, amending, adding, deleting, extracting, storing, disclosing or destroying information.

Data Integrity
The school undertakes to ensure data integrity by the following methods:

Data Accuracy

Data held will be as accurate and up to date as is reasonably possible. If a Data subject informs the school of a change of circumstances their computer record will be updated as soon as is practicable. A printout of their data record will be provided to data subjects every 12 months so they can check its accuracy and make any amendments.

Where a data subject challenges the accuracy of their data, the school will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we will try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Governing Body for their judgement. Until resolved the affected information will contain both versions.

Data Adequacy and Relevance

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the school will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

Length of Time

Data held about individuals will not be kept for longer than necessary for the purposes registered. Please refer to the appropriate Privacy notice.

The school will, in general, only disclose data about individuals with their consent. However there are circumstances under which the school's authorised officer may need to disclose data without explicit consent for that occasion. These circumstances are strictly limited. The school will not disclose anything on pupils' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything which suggests that they are, or have been, either the subject of or at risk of child abuse.

A **"legal disclosure"** is the release of personal information from the computer to someone who requires the information to do his or her job within or for the school, provided that the purpose of that information has been registered.

An **"illegal disclosure"** is the release of information to someone who does not need it, or has no right to it, or one which falls outside the school's registered purposes.

Registered Purposes

The Data Protection Registration entries for the school are available for inspection, by appointment at the school office. The current registration is held under ICO (Information Commissioner's Office) is recorded under reference Z800140X.

The Head Teacher is the person nominated to deal with Data Protection issues in the school.

Staff Responsibilities

All staff will:

- Ensure that all personal information which they provide to the school in connection with their employment is accurate and up-to-date
- Inform the school of any changes to information, for example, changes of address, changes to contact details
- Check the information which the school will make available on an annual basis, in written or automated form, and inform the school of any changes/errors

The school will not be responsible for errors of which it has not been informed.

When staff hold or process information about pupils, colleagues or other data subjects (for example pupil's assessment details, pastoral files, or details of personal circumstances), they will comply with the Data Protection Guidelines. Staff will therefore ensure that:

- All personal information is kept securely
- Such information is not disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party
- Once information is not required it must be disposed of in a secure manner, shredding.

Unauthorised disclosure may be a disciplinary matter, and may be considered gross misconduct.

Staff will be advised on an annual basis of any changes or amendments to this policy or any guidelines, as well as good practice.

Parental/Carer Responsibilities
All parents/carers will:

- Ensure that all personal information which they provide to the school is accurate and up-to-date
- Inform the school of any changes to that information, for example, changes of address, changes to contact details
- Check the information which the school will make available annually, in written or automated form, and inform the school of any errors.

The school will not be held responsible for errors of which it has not been informed.

Rights to Access Information
Staff, pupils, parents/carers and other data subjects in the school has the right to access any personal data that is being kept about them either on computer or in structured and accessible manual files. Any person may exercise this right by submitting a request to the Head Teacher by completing Appendix 1: Subject Access Request Record. The school aims to comply with requests for access to personal information as quickly as possible, but will ensure that a response is provided within 21 days unless there is good reason for the delay. In such cases, the reason for the delay will be explained in writing by the Head Teacher to the data subject making the request. All data access requests will be logged and securely filed by the School Business Manager.

Subject Consent and Sensitive Information
In some cases, such as the handling of sensitive information, the school is entitled to process personal data only with the consent of the individual. Agreement to the school processing some specified classes of personal data is a condition of admission to the school, and a condition of employment for staff.

The school may process sensitive information about a person's health, disabilities, criminal convictions, race or ethnic origin, or trade union membership. The majority of jobs within the school will bring staff into contact with children, including young people between the ages of 16 and 19, and the school has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job. The school may also require such information for the administration of the absence policy, the equal opportunities policy, and other school policies or for academic assessment.

The school also asks for information about particular health and medical needs and particular forms of medication etc. The school will use such information to protect the health and safety of the individual, for example in the event of a medical emergency.

The school will ask parents for permission to be able to take and produce photographs which may be used on the website or in newsletters /promotional material but the school will not produce information without their consent.

For further information on the data that the school may hold please refer to the appropriate Privacy Notice.

Data Protection Breach Record
If a data breach has occurred it must be reported to either the DPO or the Head Teacher as soon as possible. Using Appendix 2: Data Breach Record, it is the responsibility of the DPO / Head Teacher to report the matter to the ICO (Information commissioner's Office)

Records should be kept and retained in the school and brought to the attention of the Governing Body.

The Data Protection Officer, the Data Controller and the Designated Data Controllers
When the General Data Protection Regulations are introduced a (DPO) Data Protection Officer will be appointed to oversee the processes within the school. The school is the data controller under the Act, and the Head Teacher is ultimately responsible for implementation. Responsibility for day-to-day matters will be delegated to nominated members of staff as designated data controllers – the School Business Manager and members of the Admin Team. Information and advice about the holding and processing of personal information is available from the designated data controllers.

Standard Publication of Information
The school will not publish information into the public forum of any data classes specified in our Registry Entry without the specific permission of the individuals involved. The school, or associated third parties, will only publish digital or materials-based photographic or video sources in compliance with permissions received from individuals and parents/carers.

Information Security
The school undertakes to ensure security of personal data by the following general methods:

- Overall security policy for data is determined by the Head Teacher and is monitored and reviewed regularly. Any concerns or queries about security of data should in the first instance be referred to the Head Teacher.
- Only authorised persons are permitted to access the School's Management Information Systems. Personal information held on the Management Information Systems is password protected and access limited to specific staff members. Personal information held on computer systems should be adequately password protected. Information should never be left up on a screen if the computer is unattended.
- Disks and printouts are locked away securely when not in use. Security software is installed on all computers containing personal data. Only authorised users are allowed access to the network and password changes are regularly undertaken. Computer files are backed up (i.e. security copies are taken) regularly.
- All manual personal data will be kept in lockable filing cabinets which are kept locked when the room is unattended. Personal information should not be left on a desk where anyone could see it.
- Archived information should be stored in a lockable area – see Records Management Policy.
- Where possible personal information should not be sent by e-mail as its security cannot be guaranteed. Where possible use a 'safe haven' scan. Never send personal information in the text of an email, if necessary make sure the information is in an MS Office document attached to the e-mail. When posting information ensure the envelope is sealed.
- Be careful of giving out personal information over the telephone, unless approved by a senior member of staff; invite the caller to put the request in writing. If the request is urgent take the caller's name and switchboard telephone number and verify their details before responding.
- Do not discuss other people's personal business in public areas where conversations can be overheard by people with no right to know the details of the information.
- Appropriate building security measures are in place, such as alarms, window locks etc. Visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied.
- Do not post any information on staff or pupils in relation to personal date (see Social Media\Facebook advice)

One of the best rules of thumb for dealing with sensitive, personal information is to ask the question "if this was my information would I be happy with the way in which it is being treated?"

Enquiries
Information about the school's Data Protection Policy is available from the Head Teacher or the School Business Manager. General information about the Data Protection Act can be obtained from the Data Protection Commissioner (Information Line 01625 545745, **www.ico.gov.uk**. From the 25th May 2018 the General Data Protection Regulations (GDPR) are introduced please refer to **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/** or should you have any general questions the following website may be useful: **https://ico.org.uk/for-the-public/**

Revision Record of Published Versions			
Author	**Creation Date**	**Version**	**Status**
School	September 2014	1.0	Pending Governor Approval
	October 2014		Approved
Amended by	**Revision Date**		
School	September 2015		Approved
To be reviewed	September 2017		Pending in view of GDPR changes
HT & SBM	February 2018	1.0	Approved
To be reviewed	July 2019		Annual review no changes

Appendix 1 - Data Protection Breach Record

DATA PROTECTION BREACH

Date:

Person responsible for dealing with breach:

Outline of breach	
Which data subjects (s) are involved	
Data type involved	
Reported by	
Phone/email sent to HT / DPO	Is this high risk? Yes ☐ No ☐ Report to ICO Yes ☐ No ☐
Data reported to data subjects	
Action taken	
Preventative action suggestions including training	
Notes	

Actions approved by: _____

Date: _____/_____/_____

Appendix 2 Subject Access Request Record

SUBJECT ACCESS REQUEST RECORD

Name of data subject:

Name of person who made the request:

Date request received:

Contact HT / DPO:

Date acknowledgement sent:

Name of person dealing with request:

Questions (complete answers)	**Notes**
Are they entitled to the data	If no reply stating reasons and/or ask for proof
Do you understand what data they are asking for?	If no , ask requestor for clarity
Identify the data	What data sources where they are kept?
Collect the data required	You may need to ask others – state a deadline in your request
Do you own the data?	If no, ask third parties to release external data. If data is supplied by another agency, you do not own the data
Do you need to exempt/redact data	If exempting/redacting be clear of your reasons for delay and asking if they would like the data you have collected so far
Is the data going to be ready in time?	Record delays and reasons. Communicate with requestor stating reasons for delays and asking if they would like the data you have collected so far
Create pack	Make sure that the data is in an easy to access format: paper or computerised.
Inform requestor you have the data	Ask them how they would like it delivered
Deliver data	Ask for confirmation/special delivery

Data request completed: _____/_____/_____
(Within 30 days of request)

Signed off by: _____