

Data Protection Policy 2017

**LOW ASH PRIMARY
SCHOOL**

JANUARY 2017

The Governing Body is responsible for implementation of this Data Protection Policy. The purpose of this policy is to make you aware of how we handle your personal data.

1. Background

The Data Protection Act 1998 (DP Act (as amended)) (as amended) is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

Low Ash Primary School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

The Governing Body of the School as a corporate body is the Data Controller under the DP Act (as amended) and has a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the personal information it holds and its use. These details are then available on the ICO's website at the following link:

http://www.ico.gov.uk/what_we_cover/promoting_data_privacy/keeping_the_register.aspx

The School must also let you know how we use your information and we issue a Privacy Notice to all pupils/parents; this summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

2. Scope

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

The School collects a large amount of personal data every year including: staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data used by the School. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998 (as amended), and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

Compliance with the DP Act (as amended) is the responsibility of all members of the School. Any deliberate breach of the Data Protection Act or this policy may lead to disciplinary action being taken, or even to a criminal prosecution

3. The Eight Principles

The DP Act (as amended) lists eight data protection principles, or rules for 'good information handling'.

1. Personal data must be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specific and lawful purposes and shall not be further processed in a manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.
4. Personal data shall be accurate and where necessary kept up to date.

5. Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under the 1998 Data Protection Act.
7. 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.
8. Personal data shall not be transferred to a country outside the EEA, 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 School will comply with the eight principles at all times. This means that the school will:

- inform Data Subjects, this could be pupils, parents or staff why they need their personal information, how they will use it and with whom it may be shared. This is known as a Privacy Notice (attached).
- check the quality and accuracy of the information held
- ensure that when information is authorised for disposal it is securely destroyed
- ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system
- only share personal information with others when it is necessary and legally appropriate to do so
- set out clear procedures for responding to requests for access to personal information known as subject access in the Data Protection Act
- train all staff so that they are aware of their responsibilities and of the schools relevant policies and procedures

4. **The Data Controller and the Designated Data Controllers**

The Governing Body of the School as a corporate body is the Data Controller under the DP Act (as amended), and the Governing Body is therefore ultimately responsible for compliance with the DP Act (as amended). However, the Designated Data Controllers will deal with day to day matters. The School has four Designated Data Controllers: They are the Headteacher, Business Manager, the admin assistant and the ICT Manager.

Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the appropriate Designated Data Controller, who would be the Headteacher.

5. **Responsibilities**

The Governing Body has overall responsibility for compliance with the DP Act (as amended)

The Headteacher is responsible for ensuring compliance with DP Act (as amended) and this policy within the day to day activities of the School including appropriate training is provided for all staff and Governors.

All staff are responsible for:

- Checking that any information that they provide to the School in connection with their employment is accurate and up to date.
- Informing the School of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The School cannot be held responsible for any errors unless the staff member has informed the School of such changes.
- If and when, as part of their responsibilities, staff collect information about other people (e.g. about a pupil's assessment data, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the DP Act (as amended).

- Every member of staff and Governor involved with the collection, processing and disclosure of personal data must be aware of their duties and responsibilities by adhering to this policy and to comply with the DP Act (as amended).

ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

Your personal data will only be processed to the extent that it is necessary for the specific purposes notified to you.

ACCURATE DATA

We will keep the personal data we store about you accurate and up to date. Data that is inaccurate or out of date will be destroyed. Please notify us if your personal details change or if you become aware of any inaccuracies in the personal data we hold about you.

DATA RETENTION

We will not keep your personal data for longer than is necessary for the purpose. This means that data will be destroyed or erased from our systems when it is no longer required. [For guidance on how long certain data is likely to be kept before being destroyed, contact the School Business Manager.

PROCESSING IN LINE WITH YOUR RIGHTS

You have the right to:

- Request access to any personal data we hold about you.
- Prevent the processing of your data for direct-marketing purposes.
- Ask to have inaccurate data held about you amended.
- Prevent processing that is likely to cause unwarranted substantial damage or distress to you or anyone else.
- Object to any decision that significantly affects you being taken solely by a computer or other automated process.

DATA SECURITY

- We will ensure that appropriate measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.
- We have in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. We will only transfer personal data to a third party if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.
- Maintaining data security means guaranteeing the confidentiality, integrity and availability (for authorised purposes) of the personal data.

PROVIDING INFORMATION TO THIRD PARTIES

We will not disclose your personal data to a third party without your consent unless we are satisfied that they are legally entitled to the data. Where we do disclose your personal data to a third party, we will have regard to the eight data protection principles.

SUBJECT ACCESS REQUESTS

If you wish to know what personal data we hold about you, you must make the request in writing. All such written requests should be forwarded to the Headteacher.

The School aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days, as required by the DP Act (as amended).

As a general guide, a child of 12 or older is expected to be mature enough to make this kind of request

6. Accessing pupils' information

Pupils attending any type of school have a right of access under the DP Act (as amended) to their own information. This is known as the right of subject access. When a child cannot act for themselves or the child gives permission, parents will be able to access this information on their behalf.

If the child attends a maintained school, parents have an independent right of access to their child's educational record, under separate education regulations. A request for an educational record must receive a response within 15 school days.

7. Consent

In many cases, the School can only process personal data with the consent of the individual.

In some cases, if the data is sensitive, as defined in the DP Act (as amended), express consent must be obtained. Agreement to the school processing some specified classes of personal data is a condition of acceptance of employment for staff. This includes information about previous criminal convictions.

The School has a duty of care to all staff and students and must therefore make sure that employees and those who use School facilities do not pose a threat or danger to other users. The School may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes. The School will only use this information in the protection of the health and safety of the individual, but will need consent to process this data in the event of a medical emergency, for example.

8. Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, or race. This may be to ensure that the School is a safe place for everyone. Because this information is considered sensitive under the DP Act (as amended), staff (and pupils where appropriate) will be asked to give their explicit consent for the School to process this data. An offer of employment may be withdrawn if an individual refuses to consent to this without good reason.

9. Examples of Personal data

Definitions of personal data are highly complex, and it is difficult to define categorically. However, broadly speaking and in day-to-day use, 'personal data' is information which relates to a living, identifiable individual.

In the context of this policy and the School's requirement to process 'personal data' as part of its duty of care and to educate its pupils, 'personal data' may include:

- school admission and attendance registers;

- pupil's curricular records;
- reports to parents on the achievements of their children;
- records in connection with pupils entered for prescribed public examinations;
- staff records, including payroll records;
- pupil behaviour records;
- personal information for teaching purposes;
- records of contractors and suppliers.

If it is necessary for the School to process certain personal data to fulfil its obligations to pupils and their parents or guardians then consent is not required. However, any information which falls under the definition of personal data, and is not otherwise exempt (see below), will remain confidential. Data will only be disclosed to third parties with the consent of the appropriate individual or under the terms of this policy.

Sensitive data may include:

- ethnic or racial origin
- political opinions
- religious beliefs
- other beliefs of a similar nature
- membership of a trade union
- physical or mental health or condition
- offence or alleged offence
- proceedings or court sentence

Where sensitive personal data is processed by the School, the explicit consent in writing of the appropriate individual will be obtained.

10. Exemptions

There are a number of exemptions contained in the DP Act (as amended). These may apply to the right of subject access or to the duty to comply with one or all of the principles. Examples of exemptions include:

- crime and taxation
- parliamentary privilege
- research, history and statistics
- confidential references
- legal professional privilege

There are other exemptions under the DP Act (as amended) and would advise you seek legal advice when applying these.

11. Breach of Data Protection

If a breach occurs for example post sent to wrong address with pupil personal information, the School must deal with a breach effectively. The breach may arise from a theft, a deliberate attack on systems, from the unauthorised use of personal data by a member of staff, or from accidental loss or equipment failure. However the breach occurs Low Ash Primary School will respond to and manage the incident appropriately.

Assessing the risks Low Ash Primary School should assess any risks associated with the breach, as these are likely to affect the action taken once the breach has been contained. In particular, the school will assess the adverse consequences for individuals; how serious or substantial these are; and how likely they are to happen.

Notification of breaches – informing people about an information security breach can be an important part of managing the incident, but it is not an end in itself.

Low Ash Primary School should be clear about who needs to be notified and why. We should, for example, consider notifying the individuals concerned; the ICO; other regulatory bodies; other third parties such as the police and the banks; or the media.

Evaluation and response – it is important that Low Ash Primary School investigates the causes of the breach and records all actions taken. Also evaluate the effectiveness of our response to it. If necessary, policies and procedures should be updated accordingly.

Retention of Data

The School is required to retain staff and student personal data for a specified period of time following their departure from the School. Different categories of data will be retained for different periods of time. The relevant retention periods are available on request from the School.

12. Relationship with FOIA

Requests for access to personal data that are made by someone who is not the subject of that personal data are not subject access requests. These should be considered under the Freedom of Information Act 2000 (as amended), but the personal information will not be disclosed if doing so will breach one of the data protection principles.

13. Feedback and Complaints

We welcome any comments or suggestions you may have about the policy. If you want to make any comments about this policy or if you require further assistance or wish to make a complaint then initially this should be addressed to the Headteacher: Mr T Woollin, Low Ash Primary School, Wrose Road, Shipley BD18 1AA.

14. For advice and assistance please contact Mr T Woollin

This policy will be reviewed as it is deemed appropriate to reflect best practice or amendments made to the legislation, but no less frequently than every 2 years. The policy review will be undertaken by the Headteacher, or nominated representative

15. Information Commissioner's Office

If you are not satisfied with the assistance that you get or if we have not been able to resolve your complaint and you feel that a formal complaint needs to be made then this should be addressed to the Information Commissioner's Office. This is the independent official body that ensures compliance with the Data Protection Act 1998, Freedom of Information Act 2000 and Environmental Information Regulation and that deals with formal complaints. They can be contacted at:

Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

For your complaint to be eligible for further consideration they will usually need you to provide them with supporting information or evidence. If you are still unsure what supporting evidence you will need to send to them, are not able to provide the information they need, or are unable to complete a form, please contact their Helpline on 0303 123 1113. Call us between 9am and 5pm Monday to Friday.

Telephone: (From the UK) 0303 123 1113 or 01625 545745

E-mail: First Contact team at casework@ico.gsi.gov.uk

Website: <https://www.ico.gov.uk>

Policy adopted 25th January 2017 – Full Governing Body Meeting Resource Meeting

Signed:..... Chair of Full Governing Body

Next Review Date: January 2018