# Data Protection Policy

| | |
|---|---|
| **School:** | **Withernsea Primary Academy Trust** |
| **Effective Date:** | **1st Sept 2015** |
| **Date Reviewed:** | **September 2016** |
| **Date Due for Review:** | **September 2017** |
| **Contact Officer:** | **Nina Siddle** |
| **Contact Number:** | **01964 612800** |

## 1. Background

It is Withernsea Primary Academy Trust obligation to ensure compliance with the Data Protection Act 1998. The Information Commissioner, who oversees compliance and promotes good practice, requires all organisations, and individuals, who process personal data, to comply with the eight data protection principles.

These are:

1. Personal data shall be processed fairly and lawfully
2. Personal data shall be obtained only for one or more specified and lawful purposes
3. Personal data shall be adequate, relevant and not excessive
4. Personal data shall be accurate and, where necessary kept up to date
5. Personal data shall not be kept for longer than is necessary
6. Personal data shall be processed in accordance with the rights of data subjects, including the rights to access information (Subject Access Request)
7. Personal data will be kept in an appropriately controlled and secure environment
8. Transfers outside of the European Economic Area require adequate levels of protection

The Act also requires all organisations, and individuals, who process personal information, to register with the Information Commissioner's Office. This process is called Notification. The school is required to review their notification on an annual basis.

Data Protection law and policy aims to ensure that individual's rights and freedoms are protected. Using personal data to abuse, discriminate, or deny access to services is unlawful. The school is committed to ensuring that the personal data that it holds are used fairly and lawfully and in a non- discriminatory manner.

This policy applies to all personal data held by the school. It encompasses manual/paper records and personal data electronically processed including information gathered on CCTV systems, of whatever type and at whatever location, for use by, or on behalf of, the school.

This policy will be reviewed on a biennial basis to ensure that it reflects changes to existing

legislation, and any new legislation.

## 2. Definitions for the Purposes of this Policy:

For a breakdown of definitions please see Appendix 1.

## 3. Policy Statement

In order to operate efficiently, Withernsea Primary Academy Trust has to collect and use information about people with whom it works. These may include current, past and prospective pupils, employees, and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government. This personal information must be handled and dealt with properly; however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the Act to ensure this.

Withernsea Primary Academy Trust regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the school and those with whom it carries out business. The school will ensure that it treats personal information lawfully and correctly.

To this end the school fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998.

## 4. Scope

Withernsea Primary Academy Trust is a data controller under the Data Protection Act 1998.

This policy applies to all employees, governors, contractors, agents and representatives and temporary staff working for or on behalf of the school. The Data Protection Act does not apply to access to information about deceased individuals.

This policy applies to all personal information created or held by the school in whatever format (e.g. paper, electronic, email, microfiche, film) and however it is stored, (for example ICT system/database, shared drive filing structure, email, filing cabinet, shelving and personal filing drawers).

It is the responsibility of the Governors to ensure compliance with the Data Protection Act. However the Head Teacher is responsible for ensuring compliance with the Data Protection Act and this policy within the day to day activities of the school. The Head Teacher is responsible for ensuring that appropriate training is provided for all staff.

All members of staff or contractors who hold or collect personal data are responsible for their own compliance with the Data Protection Act and must ensure that personal information is kept and processed in-line with the Data Protection Act.

## 5. Access Rights

An individual may request to see any data held about them, or information about the reasons it is kept and processed. This is called a Subject Access Request under the Data Protection Act 1998

An adult with parental responsibility can access the information about their child, as long as the child is not considered to be sufficiently mature. They must be able to prove their parental responsibility and the school is entitled to request relevant documentation to evidence this as well as the identity of the requestor and child.

In relation to the capacity of a child to make a subject access request, guidance provided by the Information Commissioner's Office has been that by the age of 12 a child can be expected to have sufficient maturity to understand the nature of the request. A child may of course reach sufficient maturity earlier; each child should be judged on a case by case basis.

In addition, parents have their own independent right under The Education (Pupil Information) (England) Regulations 2006 of access to the official education records of their children. Students do not have a right to prevent their parents from obtaining a copy of their school records.

## 6. Information Sharing

Before sharing personal information it is the responsibility of individual members of staff to ensure that they have the authority to do so and that the recipient is authorised to receive such information. Failure to do so could lead to action under the Academy disciplinary procedure (and, in exceptional circumstances, in criminal charges).

There is a Humber Information Sharing Charter which should be referred to when considering sharing data.

## 7. Key Business Processes

When designing new business processes (including forms which are designed for the collection of data) this policy must be considered.

When changes or amendments are made to the above point, Data Protection compliance must be reviewed.

## 8. Data Quality, Integrity and Retention

In order to process personal information, the data controller must have a legitimate reason such as consent; this can be gained through the use of a fair processing notice, stipulating how their collected personal data will be used.

If an individual complains that the personal data held about them is wrong, incomplete or inaccurate, the position should be investigated thoroughly including checking with the source of the

information. In the meantime a caution should be marked on the person's file that there is a question mark over the accuracy.

If data are held for any other purposes, an individual may request that processing ceases if it is causing them unwarranted harm or distress. This does not apply if they have given their consent, if the data are held in connection with a contract with the person, if the school is fulfilling a legal requirement or if the person's vital interests are being protected. Valid written requests must be responded to in writing within 21 days.

Procedures should be in place in order to ensure that personal data are accurate, and that wherever possible, the record is kept up to date.

## 9. Breaches

The school will always treat any data breach as a serious issue. In the event of a breach, or suspected breach, the first action would be to contact Mrs. A. Harper (Headteacher) and a decision taken as to whether the ICO should be notified. In addition HR should be informed to ensure appropriate investigation is undertaken in accordance with the Academy's disciplinary policy. The Information Commissioner's Office has the authority to sanction significant financial penalties, of up to £500,000 in relation to breaches of any of the data protection principles.

## 10. Training

It is the schools policy that all employees who hold or process personal data receive the appropriate training in order to comply with the Data Protection Act 1998. Training in Data Protection matters should be provided before any access to personal data is permitted, and mandatory refresher training should be undertaken at intervals thereafter to maintain awareness. All new employees must complete an induction form, which includes a section on the Data Protection Act 1998. It is the responsibility of the managers of temporary or contracted staff to ensure they are aware of this Data Protection policy and their responsibility to adhere to it.

Data Protection training is a crucial element of staff awareness. All individuals need to be aware of their obligations relating to any personal data they process as part of their school duties. Failure to adhere to the eight data protection principles can lead to serious misconduct and prosecution.

An e-learning package is used to implement training and a record held on the Academy's central record. Staff newsletters can be used as a tool with which to remind staff of their responsibilities.

## 11. Complaints

An individual has the right to complain about the response they have received regarding their request for information as well as to complain about other breaches of the Data Protection Act. Details of the complaints procedure can be obtained from the school office and one the school website.

## 12. Photographs

Whether or not a photograph comes under the Data Protection Act is a matter of interpretation and quality of the photograph. However, the school takes the matter extremely seriously and seeks to obtain parents' permission for the use of photographs outside the school and, in particular, to record their wishes if they do not want photographs to be taken of their children.

## 13. Outcomes and impacts

- Minimise the inappropriate use of personal data held on school systems.
- Employees are aware of their responsibilities for handling personal data and that failure to do so could result in disciplinary proceedings.
- Employees are aware of their duties under the Data Protection Act, and who to contact for advice.
- Managers identify training requirements in association with handling personal data.
- Requests for personal data are handled in accordance with the Data Protection Policy.
- Third party data processors working on behalf of the school will handle personal data in accordance with the Data Protection Policy.
- The Head Teacher is made aware of all and will formally log Data Protection Act breaches and their outcomes, and will inform the ICO as appropriate.
- The school is compliant with the Data Protection Act.

## 14. Policy Implementation

The Data Protection Policy will be implemented through: staff induction process from Sept 15 onward, the review of our Single central Record for training renewals, Staff newsletters, Governor approval at policy review stage and availability on the Governor portal of the school website, available for all staff to access via the staff shared area (policies)

## 15. Evaluation

The Data Protection Policy will be subject to a review every year or earlier if required to ensure that it is appropriate and responsive to all relevant legislation and guidance.

## 16. References

Data Protection Act 1998
ICO website
ICO website – Data Controllers List

## APPENDIX 1: Definitions for the Purposes of this Policy:

For the purposes of this policy, the following definitions are in relation to Data Protection.

The school has adopted the following definitions as set out by the Information Commissioner:

**Data** means information which –

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
(b) is recorded with the intention that it should be processed by means of such equipment,
(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68[1], or
(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

**Personal data** means data which relate to a living individual who can be identified –

(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

**Sensitive personal data** means personal data consisting of information as to -

(a) the racial or ethnic origin of the data subject,
(b) an individual's political opinions,
(c) an individual's religious beliefs or other beliefs of a similar nature,
(d) whether an individual is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation Act 1992),
(e) an individual's physical or mental health or condition,
(f) an individual's sexual life,
(g) the commission or alleged commission by an individual of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by an individual, the disposal of such proceedings or the sentence of any court in such proceedings.

[1] 68 Meaning of "accessible record".
(1) In this Act "accessible record" means—
(a) a health record as defined by subsection (2),
(b) an educational record as defined by Schedule 11, or
(c) an accessible public record as defined by Schedule 12.
(2) In subsection (1) (a) "health record" means any record which—
(a) consists of information relating to the physical or mental health or condition of an individual, and
(b) has been made by or on behalf of a health professional in connection with the care of that individual.

**Processing**, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including –

(a) organisation, adaptation or alteration of the information or data,
(b) retrieval, consultation or use of the information or data,
(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
(d) alignment, combination, blocking, erasure or destruction of the information or data.

**Data subject** means an individual who is the subject of personal data.

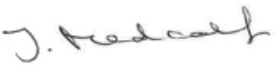
**Data controller** means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

**Data processor**, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

**Recipient**, in relation to personal data, means any person to whom the data are disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of a data processor) to whom they are disclosed in the course of processing the data for the data controller, but does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law.

**Third party**, in relation to personal data, means any person other than –

(a) the data subject,
(b) the data controller, or
(c) any data processor or other person authorised to process data for the data controller or processor.

Signed  Chair of Govs.

Signed  Headteacher