Wallace Fields Infant School and Nursery

Data Protection and Handling Policy

Wallace Fields Infant School and Nursery is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Reviewed: March 2019 **Next Review: March 2022**

Wallace Fields Infant School is proud to be a part of Inspiration Academy Trust.

Date			1st November 2015
Document Location			S:\Office\Policies\WFIS Master Policies\Data Protection and Handling Policy.docx
Policy Lead			Christina Lane
Next Review Date			March 2022
Date	Version	Amended By	Comment (e.g. reason for version change)
12.11.15	1	Christina Lane	Updated and amended policy
23.11.15	1	Ceri Jewell	Reviewed and made final edits
12.11.17	1	Christina Lane	Updated and amended policy in line with GDPR regulations
06.03.19	2	Ceri Jewell	Reviewed and made final edits
30.06.20	3	Collette Pasley	Replaced Ceri Jewell's name with Lorna Harding

Information relating to the Data Protection Policy

S:\Office\Policies\WFIS Master Policies\Data Protection and Handling Policy.docx

The Data Controller is Lorna Harding

The school Data Protection Officer is Lorna Harding

The Academy will:

- Ensure that there is a single point of contact with the overall responsibility for Data Protection (the Data Protection Officer)
- Provide awareness for all members of staff who handle personal information
- Provide clear lines of report and supervision for compliance with Data Protection
- Carry out regular checks to monitor and assesse the processing of personal data and to ensure the academy's notification to the Information Commissioner is updated to take account of any changes in processing of personal data.

Introduction

Inspiration Academy Trust is the legal entity responsible for the processing of personal data by our school. IAT is the data controller and is responsible for the processing and is entity subject to DPA registration obligations.

IAT need to collect personal information about people we work with, in order to carry out our core business of supporting learning and to provide our services. Such people include pupils, parents, Governors, employees (past, present and prospective), suppliers and other business contacts.

In addition, IAT may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law. No matter how it is collected, recorded and used (e.g. on a computer screen or on paper) this personal information must be dealt with properly to ensure compliance with the Data Protection Act 2018.

The personal information held by IAT is extremely important to ensure the success of IAT and in order to maintain the confidence of IAT pupils, parents, employees and stakeholders (identified above). IAT must ensure it treats personal information lawfully and correctly.

IAT fully supports and complies with the eight principles of the Data Protection Act 2018.

1 Adherence to the Eight Principles of the Data Protection Act 2018

1.1 Personal data shall be processed fairly and lawfully**.**
Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the Data Controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.

1.2 Personal data shall be obtained only for one or more specified lawful purposes and shall not be further processed in any manner incompatible with the purpose of those purposes.
Data obtained for specified purposes must only be used for those purposes identified.

1.3 Personal data shall be adequate, relevant and not excessive.
Information which is not strictly necessary for the purpose of which it is obtained should not be collected. If data is given or obtained which is excessive to the purpose it should be immediately deleted or destroyed.

1.4 Personal data shall be accurate and where necessary, kept up to date.
Data which is kept for a long time must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate. It is the responsibility of individuals to ensure that data held by IAT is accurate and up to date. Individuals should notify IAT of any changes in circumstances to enable personal records to be updated accordingly. It is the responsibility of IAT to ensure any notification regarding change of circumstances is noted and acted upon.

1.5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for the purpose or purposes.
IAT discourages the retention of personal data for longer than is required. Considerable amounts of data are collected on current staff and pupils. Once a member of staff or pupil has left IAT, it will not be necessary to retain all the information held on them. Some data will kept for longer periods than others.

Staff and pupil information will be retained for the time periods set out by the Information and Records Management Policy. This reflects statutory requirements and recommendations for best practice.

1.6 Personal data shall be processed in accordance with the rights of data subjects under this Act.
Data subjects have the following rights regarding data processing and the data that is recorded about them:

- *A right of access to a copy of the information comprised in their personal data*
- *A right to object to processing that is likely to cause or is causing damage or distress*
- *A right to prevent processing for direct marketing*

- *A right to object to decisions being taken by automated means*
- *A right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed*
- *A right to claim compensation for damages caused by a breach of this Act.*

1.7 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.

All staff are responsible for ensuring that any personal data (on others) which they hold is kept securely and that it is not disclosed to any unauthorised third party.

All personal data should be accessible only to those who need to use it. You should form a judgement based upon the sensitivity and value of the information in questions, but always consider keeping personal data, examples might be data should be kept:

- *In a lockable room with controlled access*
- *In a locked drawer or filing cabinet*
- *Password protected if in electronic format*
- *Securely electronically (e.g. secure back-ups).*

Care should be taken to ensure that electronic device screens are not visible except to authorised staff and that passwords are kept confidential. Electronic devices should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised persons. Personal information should not be kept on external hard drives or USB drives.

Care must be taken to ensure that appropriate security measures are in place for the deletion and disposal of personal data. Manual records should be shredded or disposed of as confidential waste. Hard drives or redundant electronic devices should be wiped clean before disposal.

This policy also applies to staff who process personal data off-site. Off-site processing presents potentially greater risk of loss, theft or damage to personal data. Staff should take particular care when processing data at home or in other locations.

Data Breach and reporting incidents

Logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy, for example.

The school has a policy for reporting, managing and recovering from information risk incidents, which establishes:
• a responsible person for each incident
• a communications plan, including escalation procedures
• and results in a plan of action for rapid resolution and
• a plan of action of non-recurrence and further awareness raising.
All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Data and computer security

Wallace Fields Infant School undertakes to ensure security of personal data by the following general methods (precise details cannot, of course, be revealed)

- *Physical security*

Appropriate building security measures are in place, such as alarms, window bars, deadlocks and computer hardware cable locks. Disks, tapes and printouts are locked away securely when not in use. Visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied.

- *Logical security*

Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up (ie security copies are taken) regularly. Personal and sensitive data should only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods). Auto lock should be enabled when devices are left unattended. Personal data can only be stored on school equipment. Private equipment must not be used for the storage of personal data. Where personal devices are used to access data remotely, passwords should not be stored on the device and personal data should not be downloaded.

- *Procedural security*

In order to be given authorised access to the computer, staff will have to undergo checks and will agree a confidentiality agreement. All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded before disposal. Overall security policy for data is determined by the Head teacher and Governing Body and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent. The School's security policy is kept in a safe place at all times. Any queries or concerns about security of data in the school should in the first instance be referred to the Headteacher. Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

1.8 Personal data shall not be transferred to a country or territory outside the European Economic Area 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.

Data must not be transferred outside of the European Economic Area (EEA) – the EU Member states together with Iceland, Liechtenstein and Norway without the explicit consent of the individual. Members of IAT should be particularly aware of this when publishing information on the internet, which can be accessed from anywhere around the globe. Transfer includes placing data on a website (or file sharing site) that can be accessed from outside of the EEA. When sensitive data is passed electronically (such as by email) between IAT and a third party it shall always be in a secure (encrypted) manner.

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 practical. A printout of their data record will be provided to data subjects every twelve 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 shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Governing Body for their judgement. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

- **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. Records are checked at the beginning of every September by sending the pupil record sheet home to parents. This amended by parents/guardians as necessary and returned to school. The information is then updated on the school computer.

- **Length of time**

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the Finance Manager to ensure that obsolete data are properly erased. The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated or otherwise disintegrated for data. A destruction Log will be maintained of all data that is disposed of. The log will include the document ID, classification, date of destruction, method and authorisation.

Subject access

The Data Protection Acts extend to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves, it is essential that a formal system of requests is in place. Where a request for subject access is received from a pupil, the school's policy is that:

Requests from pupils will be processed as any subject access request as outlined below and the copy will be given directly to the pupil, unless it is clear that the pupil does not understand the nature of the request. Requests from pupils who do not appear to understand the nature of the request will be referred to their parents or carers. Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.

Processing subject access requests

Requests for access must be made in writing.

Pupils, parents or staff may ask for a Data Subject Access form (appendix 1), available from the School Office. Completed forms should be submitted to the School Business Manager (the nominated officer). Provided that there is sufficient information to process the request, an entry will be made in the Subject Access log book, showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (eg

Student Record, Personnel Record), and the planned date of supplying the information (normally not more than 40 days from the request date). Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be date on which sufficient information has been provided.

Note: In the case of any written request from a parent regarding their own child's record, access to the record will be provided within 15 school days in accordance with the current Education (Pupil Information) Regulations.

2 CCTV

2.1 Images of people are covered by the Data Protection Act 2018 and so is information about people which is derived from images (e.g. vehicle registration numbers etc.). Ensure all procedures are followed when installing CCTV and any captured information should be processed under the principles of the Data Protection Act 2018 and this Policy. Further information about the Data Protection Code of Practice in relation to CCTV use us issued by the ICO. https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

3 IAT's Commitment

3.1 IAT will implement the requirements of the Data Protection Act 2018 and Data Retention Regulations 2018 and any subsequent amendments or regulations.

3.2 IAT will ensure that:

- The academy Data Controller will have overall responsibility for the implementation of the processes and procedures to ensure the requirements of the Data Protection Act 2018 are fulfilled
- All staff are aware of their responsibilities under the Data Protection Act 2018
- All staff are aware of their responsibilities under the Data Retention Regulations 2018
- Staff are trained and supported to adhere to the Data Protection Act 2018 including dealing with requests under Subject Access Requests
- IAT must ensure that the principles of this policy are followed for remote and/or home working, and the technology is in place to support this.

4 Monitoring

4.1 IAT will maintain a register of all requests made under the Data Protection Act 2018 that do not fall within the remit of the Data Protection Registration and the action taken for each request.

4.2 IAT will review this policy and associated procedures to ensure it remains up to date or when new legislation or regulations are released.

5 Complaints

5.1 If you are not satisfied with the response you receive from us or we have not been able to resolve your complaint and you feel that formal complaint needs to be made, then this should be addressed to the Information Commissioners' Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

6 Definitions

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 paragraphs (a), (b) or (c) but forms part of an accessible record as defined by section 68
(e) Is recorded information held by a public authority and does not fall within paragraphs (a) to (d).

Personal data means data which relate to a living individual who can be identified. This includes expressions of opinion about the individual.

Sensitive data means personal data consisting of information that could be used in a discriminatory way (e.g. racial or ethnic data) and is likely to be of a private nature. It should be treated with greater care than other personal information.

Data subject means an individual who is subject to 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.

Relevant filing system means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference ro individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

This policy links to:

- Freedom of Information Policy
- Safeguarding Policy
- Encryption Policy
- E-Safety Policy
- Social Media Policy
- CCTV Policy

(Appendix 1)
Access to personal data request

Data Protection Act 2018 Section 7.

Enquirer Surname.....Enquirer Fore Names.....

Enquirer Address .....

……

Enquirer Postcode ..... Telephone Number .....

Are you the person who is the subject of the records you are enquiring about YES / NO (i.e. the "Data Subject")?

If NO, Do you have parental responsibility for a child who is the "Data Subject" of the records you are enquiring about?

If YES, Name of child or children about whose personal data records you are enquiring
……

……

Description of Concern / Area of Concern
……

……

Description of Information or Topic(s) Requested In your own words)
……

……

Additional information

……

Please despatch Reply to: (if different from enquirer's details as stated on this form)
Name……

Address & Postcode ……

……

Data subject declaration

I request that Wallace Fields Infant School search its records based on the information supplied above under Section 7 (1) of the Data Protection Act 2018 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the School. I agree that the reply period will commence when I have supplied sufficient information to enable the School to perform the search. I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and Address above who I have authorised to receive such information).

Signature of "Data Subject" (or Subject's Parent) .....

Name of "Data Subject" (or Subject's Parent) (PRINTED).....

Dated .....