WATLING STREET PRIMARY SCHOOL

DATA PROTECTION POLICY

This document is a statement of the aims and principles of the School, for ensuring the confidentiality of sensitive information relating to staff, pupils, families and governors.

Introduction

The Governing Body of Watling Street Primary School has responsibility for ensuring that records are maintained, including security and access arrangements. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, Watling Street Primary School must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act). In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.

- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.

- Be adequate, relevant and not excessive for that purpose.

- Be accurate and kept up to date.

- Not be kept for longer than is necessary for that purpose.

- Be processed in accordance with the data subject's rights.

- Be kept safe from unauthorised access, accidental loss or destruction.

Watling Street Primary School and all staff or others who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the School has developed this Data Protection Policy.

The Data Controller and the Designated Data Controllers

The School as a body corporate is the Data Controller under the 1998 Act, and the Governors are therefore ultimately responsible for implementation. However, the Designated Data Controllers will deal with day to day matters.

The School has three Designated Data Controllers: They are the Headteacher, the Head of Business Strategy and the Senior School Administrator.

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 a Designated Data Controller.

Responsibilities of Staff

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 student's course work, opinions about ability, references to other academic institutions, or details of personal circumstances/disclosures), they must comply with the guidelines for staff set out in the Staff handbook regarding confidentiality.

Data Security

The governors recognise their responsibility to ensure that measures are taken to ensure no breach of security.
"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against loss or destruction of, or damage to, personal data."

Security of Data

As far as possible all ICT equipment is secured. Expensive portable equipment is locked away daily in the locked trolleys or other secure furniture e.g. desks, cupboards.

Personal passwords are provided to staff and pupils to enable access to curriculum networked computers. Passwords allow pupils and staff different access levels. Staff will ensure that passwords are kept confidential and changed at regular intervals. Access to management files is restricted to senior and administrative staff only.

A separate administrative server, located in the school office, is linked to the Headteacher's and Office computers and is used for confidential and personal files and systems. Access is controlled by individual passwords and limited to the Headteacher, Deputy Head and administration staff.

Controlling Access to Information

Pupil and family information will be stored using the SIMs Management Information System (MIS) on the main office administration machines. It will also be available via the network to authorised personnel. Pupil files are to be kept in a lockable filing cabinet within the main school office. Offices and rooms where data is accessible will be locked when unattended.

Staff will ensure that confidential data is not accessible or visible to visitors to the school unless they have authorisation to access that data.

Staff will not communicate via email about individual pupils.

Access to the SIMs system will be password protected and staff will ensure that passwords are kept confidential and changed at regular intervals.

The SIMs administrator will be responsible for ensuring access rights are issued to staff at a level consistent with their roles.

The SIMs MIS and curriculum server will be backed up remotely LA-ICT at a secure offsite location, on a daily basis.

Personal data will only be disclosed to authorised personnel, including: social workers, school health personnel, Walsall Children's Services. If a member of staff is unsure if data can be disclosed permission should be sought from the Headteacher or other senior manager. If there is any doubt as to the identity of a person to whom personal data may be disclosed, whether over the telephone or in person, staff must request evidence of identity. If a request is received from an authorised agency for data regarding a pupil and staff are uncertain as to the identity of the caller they should arrange to call back with the information. Any phone numbers given by other agencies should be checked to the telephone directory.

Pupil data files must not be removed from the school office without the permission of the Headteacher. Under no circumstances must files be removed from the school premises. If files have been taken to other rooms within the school they must not be left unattended and must be returned to the school office at the earliest opportunity.

School laptops and iPads may be used at home providing they have been updated to special privilege setting. All equipment taken off premises must be signed out in the relevant log in the school office. SIMs will not be installed on laptops that are used by staff at home.

Appropriate building security measures are in place, including alarm systems, key pad entry to the school. Offices are locked when unattended.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should:

- Be kept in a locked filing cabinet, drawer, or safe; or

- If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up; and

- If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Staff Selection and Training

All appointed staff will be expected to be honest and trustworthy and to show discretion and integrity. References will be taken up for all shortlisted candidates.

Relevant staff will receive instruction and training with regard to their responsibilities in connection with data protection.

Failure to comply with confidentiality and data protection may result in a formal warning for staff employed at the school in any capacity and further measures being considered by the Governors, including access to personal data being withdrawn.

All students on placement at school must be informed about how to deal with confidential matters. The Headteacher reserves the right to withdraw the training place granted to a student on placement who breaks confidentiality and voluntary workers will no longer be invited into school.

Data must only be accessed for legitimate school business and not for private purposes.

Detecting and Dealing with Breaches of Security

The SIMs MIS keeps an audit trail of all entries and amendments and identifies the user.

The Head of Business Strategy will be responsible for ensuring the security of the management information system (SIMs). The Head of Business Strategy and Senior School Administrator will ensure that all data entered or amended is accurate. No other staff will have access rights to enter or amend data. Breaches of security will be investigated and the necessary action will be taken to rectify or remedy the situation.

All data will be processed by trained employees of Watling Street Primary School or Walsall Children’s Services Information Services and Data Team personnel.

The data controller must have regard to the obligations placed upon them by The Act in respect of processing of personal data by a data processor. In order to comply with the Seventh Principle the data controller must:*

- *choose a data processor providing sufficient guarantees in respect of the technical and organisational security measure they take*

- *take reasonable steps to ensure compliance with those measures; and*

- *ensure that the processing by the data processor is carried out under a contract, which is made or evidenced in writing, under which the data processor is to act only on instructions from the data controller. The contract must require the data processor to comply with obligations equivalent to those imposed on the data controller by the Seventh Principle.*

The above is an extract from 'The data Protection Act 1998 – Legal Guidance'

*"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," e.g. Data Team, IMS Team, QCA etc.

Other data protection issues:

- Printed material is disposed of by shredding in accordance with retention guidelines

- Staff diaries and record books are shredded at the end of the academic year

- Parents are informed of data kept in school and its use through the Fair Processing Notice

- Emergency and Business Continuity Plan is in place

- School anti-virus software is updated daily

- School telephone conversations are not recorded

Rights to Access Information

All staff, parents and other users are entitled to:

- Know what information the School holds and processes about them or their child and why.

- Know how to gain access to it.

- Know how to keep it up to date.

- Know what the School is doing to comply with its obligations under the 1998 Act.

This Policy document and the School's Fair Processing Notice address in particular the last three points above. To address the first point, the School will, upon request, provide all staff and parents and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the School holds and processes about them, and the reasons for which they are processed.

All staff, parents and other users have a right under the 1998 Act to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should contact the Designated Data Controller.

The School may make a charge on each occasion that access is requested.

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 1998 Act.

Subject 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 1998 Act, 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.

Employment will bring the applicants into contact with children. The School has a duty under the Children Act 1989, Keeping Children Safe in Education (updated 2015), and other enactments to ensure that staff are suitable for the role. 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 e.g. asthma, diabetes etc. 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.

Publication of School Information

Certain items of information relating to School staff will be made available via searchable directories on the school's internet site, in order to meet the legitimate needs of researchers, visitors and enquirers seeking to make contact with the School.

Retention of Data

The School has a duty to retain some staff and student personal data for a period of time following their departure from the School, mainly for legal reasons, but also for other purposes such as being able to provide references. Different categories of data will be retained for different periods of time in accordance with data retention guidelines.

Conclusion

Compliance with the 1998 Act is the responsibility of all members of the School. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or even to a criminal prosecution.