ALL SAINTS C OF E PRIMARY SCHOOL
NEWTON HEATH
MANCHESTER

Data Protection Policy

Updated January 2017

ALL SAINTS C OF E PRIMARY SCHOOL, NEWTON HEATH

Data Protection Policy

UPDATED JANUARY 2017

Mission Statement

Through Christian teaching, we aim to develop an inclusive learning community, where through strong relationships the achievements of all are celebrated.

This document is a statement of the aims and principles of All Saints C of E Primary School, for ensuring the confidentiality of sensitive information relating to staff, pupils, parents and governors.

INTRODUCTION

All Saints C of E Primary School needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. 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, All Saints C of E Primary School must comply with the Data Protection Principles which are set out in the Data Protection Act 1998.

In summary these state that personal data shall:
1. Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
2. Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
3. Be adequate, relevant and not excessive for that purpose.
4. Be accurate and kept up to date.
5. Not be kept for longer than is necessary for that purpose.
6. Be processed in accordance with the data subject's rights.
7. Be kept safe from unauthorised access, accidental loss or destruction.
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

All Saints C of E 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.

POLICY SCOPE

This policy applies to:
- Governing Body
- All Staff and volunteers
- All contractors, suppliers and other people working on behalf of All Saints C of E Primary School

It applies to all data that the school holds relating to identifiable individuals, even if that information technically falls outside of the data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- any other information relating to individuals

STATUS OF THIS POLICY

This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the School from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

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 two Designated Data Controllers: They are the Headteacher and School Business 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.

DATA PROTECTION RISKS

This policy helps to protect All Saints C of E Primary School from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, Information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the organisation uses data relating to them.
- **Reputational Damage.** For instance, the school could suffer if somebody unlawfully gained access to sensitive data.

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 or name. 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).

These people have key areas of responsibility:

The Headteacher, Senior Leadership team and Governing body is ultimately responsible for ensuring that All Saints C of E Primary School meets its legal obligations.

The School Business Manager is responsible for:

- Keeping the Headteacher, Senior Leadership team and Governing body updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.

- Dealing with requests from individuals to see the data All Saints C of E Primary School holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the organisation's sensitive data.

The IT Technician Manager is responsible for:
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the organisation is considering using to store or process data. For example, cloud computing and storage services.

DATA SECURITY

All staff are responsible for ensuring that:
• Any personal data that they hold is kept securely.
• Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

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 other removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.
- If stored in cloud services should be protected by a strong password.

GENERAL STAFF GUIDELINES

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- All Saints C of E Primary School will provide training to all employees to help them to understand their responsibilities when handing data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the School or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their line manager or the School Business Manager if they are unsure about any aspect of data protection.

DATA USE

Personal data is of no value to All Saints C of E Primary School unless the school can make use of it. However, it is when personal data is accessed and used that it can be at the greatest loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally.** In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The IT Technician Manager can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the EEA. (European Economic Area)**
- Employees **should not save copies of personal data to their own computers**. Always access and update the central copy of any data.

DATA ACCURACY

The law requires All Saints C of E Primary School to take reasonable steps to ensure data is kept accurate and up to date.
The more important it is that the personal data is accurate, the greater effort All Saints C of E Primary School should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as **few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated**. For instance, by confirming a person's details when they call or annually for staff.

- All Saints C of E Primary School will make it easy for data subjects to update the information All Saints C of E Primary School holds about them.
- Data should be updated as accuracies are discovered.

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 addresses 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 complete the Subject Access Request Form and submit it to the Designated Data Controller.
The School will make a charge of £10 on each occasion that access is requested, although the School has discretion to waive this.
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 4 obtained. Agreement to the School processing some specified classes of personal data is a
condition of acceptance of employment for staff. This included information about previous criminal convictions.
Jobs will bring the applicants into contact with children. The School has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job. 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.

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, or to operate other School policies, such as the Sick Pay Policy or the Equal Opportunities Policy.

Because this information is considered sensitive under the 1998 Act, staff (and students where appropriate) will be asked to give their express 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.

PUBLICATION OF SCHOOL INFORMATION

Certain items of information relating to School staff will be made available via searchable directories on the public Web 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 or academic transcripts. Different categories of data will be retained for different periods of time in accordance with the Records Management Toolkit for Schools document.

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.

SIGNED:_____(Headteacher)

Date:_____

SIGNED:_____(Chair of Governors)

Date:_____

This Policy has been ratified by the Governing Body at its meeting on Thursday, 2nd March and will be reviewed in January 2018.
It was updated in January 2017.