St Mary's Catholic Federation, Carshalton

"St Mary's is committed to being a Rights Respecting School to inspire and support the children, parents and school governors in school and the wider community."

Data Protection Policy
(Statutory)
(Annual)

This policy is to be read in conjunction with the following policies:
Safeguarding & Child Protection and Freedom of Information.

Author: Emer Allen & Shirley Hulme
Committee: Resources
Date Prepared: July 2017
Date Approved: October 2017
Date of Review: October 2018

Approved by Full Governing Body on Date:

Chair of Governors……..
St Mary's Catholic Federation, Carshalton

Safeguarding Statement
This school takes notice of and adheres to all the national and local policies and guidance in regard to Safeguarding Children and Young People.

Lead Safeguarding Person Junior School: Mrs G Owens

Lead Safeguarding Person Nursery & Infant School: Mrs M Quinn

Safeguarding Deputy: Mrs S Hulme

Governor designated safeguarding officer: Mr A Scully

General Statement

The Governing Body of the school has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.

The Headteacher and Governors of this School intend to comply fully with the requirements and principles of the Data Protection Act 1984 and the Data Protection Act 1988. All staff involved with the collection. Processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.

Enquiries

Information about the School's Data Protection Policy is available from the School Business Manager. General information about the Data Protection Act can be obtained from:
The Data Protection Commissioner Information Line helpline 0303 123 1113
Website: www.ico.org.uk
The Information Commissioner's Office (ICO) provides independent advice and guidance about data protection and freedom of information.

Fair Obtaining and Processing

St Mary's Catholic Nursery, Infant and Junior Schools undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data are held, the likely recipients of the data and the data subjects' right of access. Information about the use of personal data is printed on the appropriate collection form. If details are given verbally, the person collecting will explain the issues before obtaining the information.

"processing" means obtaining, recording or holding the information or data or carrying out any or set of operations on the information or data.

"data subject" means an individual who is the subject of personal data or the person to whom the information relates.

"personal data" means data which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, Internet or media.

"parent" has the meaning given in Education Act 1996, and includes any person having parental responsibility or care of a child.

Registered Purposes

The Data Protection Registration entries for the Schools are available for inspection, by appointment, at the school office. Explanation of any codes and categories entered is available from the Headteacher, who is the person nominated to deal with Data protection issues in the School. Registered purposes covering the data held at the school are listed on the school's Registration and data collection documents. Information held for these stated purposes will not be used for any other purpose without the data subject's consent.

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 Schools of a change of circumstances their computer record will be updated as soon as is practicable. A printout of their data record will be provided to data subjects every twelve months so they can check its accuracy and make amendments during Spring Term PAR Day.

Where a data subject challenges the accuracy of their data, the Schools 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 the principle, the Schools will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

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 Headteacher to ensure that obsolete data is properly erased.

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 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.

Parents or staff may ask for a Data Subject Access form, available from the School Office. Completed forms should be submitted to the Headteacher. 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 the 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.

Authorised Disclosures

The Schools will, in general, only disclose data about individuals with their consent. However, there are circumstances under which the School's authorised officer may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- Pupil data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations

- Pupil data disclosed to authorised recipients in respect of their child's health, safety and welfare.

- Pupil data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school.

- Staff data disclosed to relevant authorities eg in respect of payroll and administrative matters

- Unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside the school. Officers and IT personnel writing on behalf of the LA are IT liaison/ data processing officers, for example in the LA, are contractually bound not to disclose personal data.

- Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the school by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the school who **need to know** the information in order to do their work. The school will not disclose anything on pupils' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything that suggests that they are, or have been, either subject of or at risk of child abuse.

A **"legal disclosure"** is the release of personal information from the computer to someone who requires the information to do his or her job within or for the schools, provided that the purpose of that information has been registered.

An **"illegal disclosure"** is the release of information to someone who does not need it, or has no right to it, or one which falls outside the School's registered purposes.

Data and Computer Security

St Mary's Catholic Nursery, Infant and Junior School under takes 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. Only authorised persons are allowed in the school offices. 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 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.

Data in Transit (memory sticks, email, laptops etc)

- when sensitive or personal data is required by an authorised user from outside the school's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform

- if secure remote access is not possible, users must only remove or copy personal or sensitive data from the school premises if the storage media, portable or mobile device (memory stick) is encrypted and is transported securely for storage in a secure location. Council policy requires the use of a specific whole-disk encryption software called PGP Whole Disk Encryption on any laptop which is used to store confidential data.

- users must securely delete personal or sensitive data when it is no longer required.

- it's important to bear in mind that messages and attachments sent via the Internet (Email) are inherently insecure and may pass through many mail services in transit. Messages are not guaranteed to go uninspected and can be misdirected to an unintended recipient if there's an error in the email address, especially if the address has been guessed by the sender or if the receiving account has an auto-forward to another address.

- Emailing documents within the LGFL system is inherently secure, however staff should still password-protect documents because there's no telling who might forward them on without your knowledge once they've been delivered to the intended recipient. The passwords should be agreed via a different route. For more important matters, file attachments should be encrypted using a program such as WinZip- www.winzip.com

Procedural Security

In order to be given authorised access to the computer, staff will have to undergo checks and will sign a confidentiality agreement. All staff are informed of 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 Headteacher/ 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 a disciplinary matter, and serious breaches could lead to dismissal.

Taking photos/ videos in school

There have been many instances reported in the press where schools haven't allowed parents to take photographs or videos of their children in the school Nativity play. Usually, the Data Protection Act 1998 (the Act) is blamed because it strictly controls when "personal data" (such as images and other data that identifies a living individual) may be "processed" (processing includes the recording, holding and disclosure of personal data).

Does the Act apply to photographs or videos in school?

It rarely applies to taking photographs or videos in schools and, where it does, the Information Commissioner's Office (the ICO), which oversees enforcement of the Act, has advocated a common-sense application to it.

The Act notes, at Section 36, that "personal data processed by an individual only for the purposes of that individual's personal, family or household affairs (including recreational purposes)" are exempt from the Act. This would include photographs taken by family members of their children at school events.

Is there any guidance available on exactly when the Act does and does not apply?

There is. In its "Data Protection Good Practice Note" on taking photographs in schools, the ICO has given some useful examples of scenarios where the Act will not apply:

- "a parent takes a photograph of their child and some friends taking part in the school Sports Day to be put in the family photo album. These images are for personal use and the Data Protection Act does not apply".
- "grandparents are invited to the school nativity play and wish to video it. These images are for personal use and the Data Protection Act does not apply"

There are, however, instances where the Act will apply and the school (or other organisation taking the photographs or film such as a local newspaper) will need to comply with the Act. Examples are:

- A small group of pupils are photographed during a science lesson and the photo is to be used in the school prospectus. This will be personal data but will not breach the Act as long as the children and/ or their guardians are aware this is happening and the context in which the photo will be used".
- "A photograph is taken by a local newspaper of a school awards ceremony. As long as the school has agreed to this, and the children and/ or their guardians are aware that photographs of those attending the ceremony may appear in the newspaper, this will not breach the Act".

Should we be obtaining consent?

In circumstances where the Act does apply, the key obligation of schools or the relevant third party is to ensure that consent from parents (or guardians) and pupils is obtained for that photography or filming. In its Good Practice Note, the ICO advocates a common sense approach to obtaining this consent:

"a common sense approach suggests that if the photographer asks for permission to take a photograph, this will usually be enough to ensure compliance Photos taken for official school use may be covered by the Act and pupils and students should be advised why they are being taken".

What about implied consent, where parents do not object to the photo or video?

If, after being notified by the school that a pupil will be photographed or filmed (stating the reason for the photographs or film), the pupil or parent does not notify the school that they object, you can assume implied consent. It follows of course then that if a pupil, parent or guardian does object, the school should not take photographs or films of the relevant pupil on that occasion.

The School reserves the right to set parameters to restrict the use of technological equipment in school for safeguarding purposes.

ACCESS TO PERSONAL DATA REQUEST

DATA PROTECTION ACT 1998 Section 7.

Enquirer's Surname…….. Enquirer's Forenames……

Enquirer's Address ……..

……

……..

Enquirer's Postcode……

Telephone number……..

Are you the person who is the subject of the records you are enquiring about
YES/ NO

If NO,

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

If YES,

Name of child or children about whose personal data records you are enquiring

Description of Concern/ Are of Concern

Description of Information or Topic(s) requested (in your own words)

Additional information

Please dispatch reply to: (if different from the enquirer's details as stated on this form)

Name

Address

Postcode

DATA SUBJECT DECLARATION

I request that the School search its records based on the information supplied above under Section 7 (1) of the Data Protection Act 1998 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…….