ST. PATRICK'S
CATHOLIC PRIMARY SCHOOL

Data Protection Policy

Reviewed by the Governing Body April 17
To be reviewed again April 2018

MISSION STATEMENT

At St. Patrick's school we will provide excellence in education inspired by the practice of our Catholic Faith.

We will make the most of all our gifts in our safe, happy and caring school. With Jesus Christ as our friend and model, we will help each other to grow in the love of God, developing self esteem, and a love of learning.

Introduction
St. Patrick's Catholic Primary School is registered under the Data Protection Act and needs to keep certain information about its staff, parents and children. It is also necessary to process information so that employees can be recruited and paid. St. Patrick's Catholic Primary school must comply with the Data Protection Principles that are set out in the Data Protection Act 1998 and amended in 2002.

In summary these state that personal data will:

- be obtained and processed fairly and lawfully and will not be processed unless certain conditions are met
- be obtained for a specified and lawful purpose and will not be processed in any manner incompatible with that purpose
- be adequate, relevant and not excessive for those purposes
- 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
- not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation. It will apply to information regardless of the way it is collected, used,

recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

St. Patrick's School staff and all staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

Status of the policy
Any member of St. Patrick's School staff or any individual on whom the school holds information who considers that this policy has not been followed in respect of personal data about themselves, should raise the matter with the designated data controller (SBM) initially. If the matter is not resolved it should be raised as a formal grievance.

Notification of Data Held and Processed

All staff or any individual on whom the school holds information are entitled to:

- know what information St. Patrick's School holds and processes about them and why
- Know how to gain access to it
- Know how to keep it up to date
- Know what St. Patrick's is doing to comply woth its obligations under the 1998 Act

Responsibilities of Staff:

As an individual you are responsible for:

- checking that any information you provide to St. Patrick's School in connection with your employment is accurate and up to date
- informing St. Patrick's School of any changes to information which you have provided e.g. changes of address
- checking the information that St. Patrick's School will send out from time to time e.g. the yearly personal details update
- informing St. Patrick's School of any errors or changes.

St. Patrick's School cannot be held responsible for any errors unless you have informed the school of them. If, and when, as part of your responsibilities, you collect information about other people (opinions on reports, references, marks, details of personal circumstances) you should follow the guidelines set out in the introduction.

Data Security:
As an individual you are responsible for ensuring that:

- any personal data that you hold is kept securely
- personal information is not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party

Personal information should be:

- kept in a locked filing cabinet, or in a locked drawer, or
- if it is computerised, be password protected, or kept only on disk which is itself kept securely.

Rights to Access Information:

Staff or any individual on whom the school holds information at St. Patrick's School have the right to access any personal data that is being kept about them either on computer or in certain files. Anyone who wishes to exercise this right should report this to the Data Controller (SBM).
Before gaining access, the person might wish to know what information is currently being held. This request should be made in writing. The school is entitled to make a charge on each occasion that access is requested.
St. Patrick's School aims to provide access to personal information as quickly as possible, but will make sure that it is provided within 21 working days unless there is good reason for delay. In such cases, the reason for the delay will be explained in writing to the person making the request.

Subject Consent:
St. Patrick's School can only process personal data with the consent of the individual. Agreement to St. Patrick's School processing certain types of personal data is a condition of employment for staff. This includes information about previous criminal convictions.
All members of staff and volunteers who come into contact with children will be subject to DBS checks. St. Patrick's School has a duty under the Children Act and other enactments to ensure that staff are suitable for the job. We also have a duty of care to all staff and volunteers, and must, therefore, make sure that employees and those who use St. Patrick's facilities do not pose a threat or danger to other users. St. Patrick's School will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. We will only use the information in the protection of the health and safety of the individual.

Processing Sensitive Information:
When data is sensitive, **express consent** must be obtained to share the information with other specified individuals. Sometimes it is necessary to process information about a person's health, criminal convictions, race, ethnicity, gender and family details. This may be to ensure St. Patrick's School is a safe place for everyone, or to operate other St. Patrick's School policies. Because this information may be sensitive and we recognise that the processing of it may cause concern or distress, staff and students will be asked to give express consent for the college to do this.

Retention of Data:
All information will be kept for a minimum of seven years. This will include information necessary in respect of pensions, taxation and information required for job references. A full list of information with retention times is available from the Data Controller.

Disposal of information:
Printed information will be shredded. Any disks containing information will be physically destroyed and all computer information will be deleted permanently.

Conclusion:
It is the legal responsibility of all members of St. Patrick's School to ensure that they fulfil their role at the school within the terms of this policy and the legal framework for data protection. This policy lays out St. Patrick's School's obligations to you under the legal framework.

Complaints
Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Review
This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Resources Committee of the Governing Body.

Contacts
If you have any enquires in relation to this policy, please contact the Headteacher who will also act as the contact point for any subject access requests.

Rights of access to information
There are two distinct rights of access to information held by schools about pupils.
1. Under the Data Protection Act 1998 any individual has the right to make a request to access the personal information held about them.

2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (Wales) Regulations 2004.

These procedures relate to subject access requests made under the Data Protection Act 1998.

Actioning a subject access request
1. Requests for information must be made in writing; which includes email, and be addressed to **Sean Cranitch - *Headteacher*).** If the initial request does not clearly identify the information required, then further enquiries will be made.
2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

This list is not exhaustive.

3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Headteacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The school may make a charge for the provision of information, dependent upon the following:

- Should the information requested contain the educational record then the amount charged will be dependant upon the number of pages provided.

- Should the information requested be personal information that does not include any information contained within educational records schools can charge up to £10 to provide it.

- If the information requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Headteacher.

5. The response time for subject access requests, once officially received, is 40 days **(not working or school days but calendar days, irrespective of school holiday periods)**. However the 40 days will not commence until after receipt of fees or clarification of information sought

6. The Data Protection Act 1998 allows exemptions as to the provision of some information; **therefore all information will be reviewed prior to disclosure**.

7. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school.
Before disclosing third party information consent should normally be obtained.
There is still a need to adhere to the 40 day statutory timescale.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

9. If there are concerns over the disclosure of information then additional advice should be sought.

10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

12. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover.
The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

Complaints
Complaints about the above procedures should be made to the Chairperson of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.
Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Data Security Breach Management

Appropriate measures are taken against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data by the school. In the event of a data security breach for the following reasons (*this is by no means an exhaustive list):*

• Loss or theft of data or equipment on which data is stored on school premises or outside
• Inappropriate access controls allowing unauthorised use
• Equipment failure
• Human error - correspondence with personal data sent to the wrong email address
• Unforeseen circumstances such as a fire or flood
• Hacking attack
• 'Blagging' offences where information is obtained by deceit from the school

The school will follow the following steps in the event of a security breach:

Containment and recovery

- Decide on who should take the lead on investigating the breach and ensure they have the appropriate resources.
- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise
- Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause.
- Where appropriate, inform the police

Assessment of ongoing risk

The following points are also likely to be helpful in making this assessment:

- What type of data is involved – staff or pupil sensitive personal data
- Where personal data has been lost or stolen, are there any protections in place such as encryption?
- How many staff and/or pupils personal data are affected by the breach?
- What harm can be done to these individuals – risks to physical safety, reputation etc.

Notification of breach

The Information Commissioner (ICO) believes serious breaches should be brought to the attention of his Office. The school's notification to the ICO would include a description of how and when the breach occurred and what data was involved. It will also include details of what have been done to respond to the risks posed by the breach.

Evaluation and response

It is important the school investigates the causes of the breach and also evaluate the effectiveness of our response to it. If necessary, the school would update its policies and procedures accordingly.