ST. EDWARD'S CATHOLIC PRIMARY SCHOOL

PERSONAL DATA HANDLING POLICY

Adopted …….. (Chair of Governors)
Updated Spring Term 2021

Through God's Grace
We Grow And Learn

Introduction

Our school will comply with the requirements of the Data Protection Act 2018 (DPA). This policy is in place to ensure our staff and governors, who are involved with the collection, processing and disclosure of personal information have been made aware of their duties and responsibilities.

We take our Data Protection obligations, under the UK General Data Protection Regulation (GDPR), very seriously and we will ensure that our school treats personal information lawfully and correctly. We safeguard information about individuals needs and treat them with respect and ensure that it is secure. We understand that UK GDPR exists to protect individual rights in an increasingly digital world.

This policy complies with the requirements set out in UK GDPR, which came into effect on 25th May 2018.

Applicable Data

For the purpose of this policy, personal data refers to information that relates to a living person that can identify them. This can be by name, address or phone number for example. The GDPR applies to both automated personal data and to a manual filing system where personal data is accessible.

Some data is considered to be more sensitive, and therefore more important to protect. This is information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation, genetic data, and biometric data where processed to uniquely identify a person.

Schools often collect sensitive data for DfE and LA requirements and of course pupil data may contain information about safeguarding, SEN or health needs. Information about other family members may also be on the school file.

School must have a legitimate reason to hold the data, we explain this in the Data Privacy Notices on the website.

Data Protection Principles

In accordance with the requirements outlined in the UK GDPR, we demonstrate our commitment, we fully endorse and adhere to the principles of the DPA;
1. Personal data shall be processed fairly, lawfully and in a transparent manner in relation to individuals, in particular, shall not be processed unless—
(a) At least one of the conditions in Schedule 2 is met, and
(b) In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
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.
8. Personal data shall not be transferred to a country or territory outside the UK 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.
9. The UK GDPR also requires that 'the controller shall be responsible for, and able to demonstrate, compliance with the principles. For our school the Governors are the data controller. They have delegated this to data processors to act on their behalf.

In addition Schedule 2 states that processing may only be carried out where one of the following conditions has been satisfied i.e. where;

- The individual has given his/her consent to the processing
- The processing is necessary for the performance of a contract with the
- individual
- The processing is required under a legal obligation
- The processing is necessary to protect the vital interests of the individual
- The processing is necessary to carry out public functions
- The processing is necessary in order to pursue the legitimate interests of the data controller or certain third parties (unless prejudicial to the interests of the individual).

Our Commitment

Our school will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR. We will,

- Comply with the DPA principles and will provide comprehensive, clear and transparent privacy policies ;

- Ensure that everyone managing and handling personal information understands their individual and organisational obligations;

- Ensure data collected is accurate and steps are taken to check and confirm accuracy. This includes when pupils join the school and check this on an annual basis.

- Respond appropriately if a Data Subject feels that the information held is inaccurate, should not longer be held by the Controller or should not be held by the Controller in any

event a dispute resolution process and complaint process can be accessed, using the suitable forms.

- Ensure we have a retention policy that explains how long we store records for. This is available on request and is on the website.

- Ensure that everyone managing and handling personal information is appropriately trained;

- Ensure we have we have processes in place to keep data safe. That might be paper files, electronic records or other information. Refer to Data Security section.

- Respond to requests for access to personal information in accordance with the subject access provisions promptly and courteously. A form is available on our website, please see our Subject Access Request Policy or if you would like a paper copy please contact the school office.

- Ensure school is registered with the Information Commissioner's Office so that our processing of personal information is lawful.

Data Subject and their rights

Someone whose details we keep on file. Some details are more sensitive than others. The UK GDPR sets out collection of details such as health conditions and ethnicity which are more sensitive than names and phone numbers.

Data subjects' rights

Individuals have a right:-

- to be informed
- of access to data stored about them or their children
- to rectification if there is an error on the data stored
- to erasure if there is no longer a need for school to keep the data
- to restrict processing, i.e. to limit what is done with their data
- to object to data being shared or collected

Data subjects' rights are also subject to child protection and safeguarding concerns, sharing information for the prevention and detection of crime. Schools also have legal and contractual obligations to share information with organisations such as the Department for Education, Social Care, the Local Authority and HMRC amongst others. In some cases these obligations override individual rights.

Data Security

- Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.
- Confidential paper records will not be left unattended or in clear view anywhere with general access.
- Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.
- Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.
- Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

- All electronic devices are password-protected to protect the information on the device in case of theft.
- Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- Staff and governors will not use their personal laptops or computers for school purposes unless they are personally password-protected and fully encrypted
- All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.
- Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.
- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- When sending confidential information by fax, staff will always check that the recipient is correct before sending.
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.
- Before sharing data, all staff members will ensure: • They are allowed to share it. • That adequate security is in place to protect it. • Who will receive the data has been outlined in a privacy notice.
- Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.
- The physical security of the school's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.
- St Edward's Catholic Primary School takes its duties under the UK GDPR seriously and any unauthorised disclosure may result in disciplinary action.
- The school is responsible for continuity and recovery measures are in place to ensure the security of protected data.

Data Protection Officer (DPO)

We have a Data Protection Officer whose role is to:-

- to inform and advise the controller or the processor and the employees who carry out processing of their obligations under the UK GDPR
- to monitor compliance with the UK GDPR and DPA
- to provide advice where requested about the data protection impact assessment and monitor its performance
- to be the point of contact for the school's Data Compliance manager if there are concerns about data protection who will liaise with the Data Protection Officer.
- to cooperate with the supervisory authority and manage the breach procedure
- to advise about training and CPD for the UK GDPR

Our DPO is John Walker whose contact details are: 0333 7729763 john@jawalker.co.uk

J. A. Walker, Office 7, The Courtyard, Gaulby Lane, Stoughton, Leicestershire, LE2 2FF

Processing Data

School must have a reason to process the data about an individual. Our privacy notices set out how we use data. The UK GDPR has 6 conditions for lawful processing and any time we process data relating to an individual it is within one of those conditions.

If there is a data breach see Appendix 1 and Appendix 2 plus separate flowchart: we follow these to take immediate action to remedy the situation as quickly as possible.

The legal basis and authority for collecting and processing data in school are:-

- consent obtained from the data subject or their parent
- performance of a contract where the data subject is a party
- compliance with a legal obligation
- to protect the vital interests of the data subject or other associated person
- to carry out the processing that is in the public interest and/or official authority
- it is necessary for the legitimate interests of the data controller or third party
- in accordance with national law.

In addition, any special categories of personal data are processed on the grounds of

- explicit consent from the data subject or about their child
- necessary to comply with employment rights or obligations
- protection of the vital interests of the data subject or associated person
- being necessary to comply with the legitimate activities of the school
- existing personal data that has been made public by the data subject and is no longer confidential
- bringing or defending legal claims
- safeguarding
- national laws in terms of processing genetic, biometric or health data.

Processing data is recorded within the school systems.

Data Sharing

Data sharing is done within the limits set by the UK GDPR. Guidance from the Department for Education, health, the police, local authorities and other specialist organisations may be used to determine whether data is shared.

The basis for sharing or not sharing data is recorded in school.

Breaches & Non Compliance

If there is non-compliance with the policy or processes, or there is a DPA breach as described within the GDPR and DPA 2018 then the guidance set out in the Breach & Non Compliance Procedure and Process needs to be followed. (See also Appendix 1 and 2 and breach flowchart.)

Protecting data and maintaining data subjects' rights is the purpose of this policy and associated procedures.

Consent

As a school we will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required.
However, in most cases data will only be processed if explicit consent has been obtained.

Consent is defined by the UK GDPR as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

We may seek consent from young people also, and this will be dependent on the child and the reason for processing.

Consent and Renewal

On the school website we have 'Privacy Notices' that explain how data is collected and used. It is important to read those notices as it explains how data is used in detail.

Obtaining clear consent and ensuring that the consent remains in place is important for school. We also want to ensure the accuracy of that information.

For Pupils and Parents/Carers

On arrival at school you will be asked to complete a form giving next of kin details, emergency contact and other essential information. We will also ask you to give consent to use the information for other in school purposes, as set out on the data collection/consent form.

We review the contact and consent form on an annual basis. It is important to inform school if details or your decision about consent changes. A form is available on our website.

Pupil Consent Procedure

Where processing relates to a child under 16 years old, school will obtain the consent from a person who has parental responsibility for the child.

Pupils may be asked to give consent or to be consulted about how their data is obtained, shared and used in certain situations.

Withdrawal of Consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent the school will consider each situation on the merits and within the principles of GDPR and also child welfare, protection and safeguarding principles.

Please complete the appropriate form which is available on our website or from the school office.

Physical Security

In school, every secure area has individuals who are responsible for ensuring that the space is securely maintained and controlled if unoccupied, i.e. locked. Offices and cupboards that contain personal data should be secured if the processor is not present.

The Premises Manager/supervisor is responsible for authorising access to secure areas along with SLT/business Manager.

All Staff, contractors and third parties who have control over lockable areas must take due care to prevent data breaches.

Secure Disposal

When disposal of items is necessary a suitable process must be used. This is to secure the data, to provide a process that does not enable data to be shared in error, by malicious or criminal intent.

These processes, when undertaken by a third party are subject to contractual conditions to ensure GDRP and DPA compliance.

Hardware is disposed / recycled by School's ICT

Hard copy files are destroyed by School's ICT

Servers and Hard drives are cleansed by School's ICT

Portable and removable storage are destroyed / cleaned/ recycled by School's ICT

Complaints & the Information Commissioner Office (ICO)

The school Complaint Policy deals with complaints about Data protection issues.

There is a right to complain if you feel that data has been shared without consent or lawful authority

You can complain if you have asked to us to erase, rectify, not process data and we have not agreed to your request.

We will always try to resolve issues on an informal basis, and then through our formal complaints procedure. Please complete the form available on our website or from the school office and we will contact you with more details about the timescale and process.

In the UK it is the ICO who has responsibility for safeguarding and enforcing the DPA

obligations. Email: casework@ico.org.uk Helpline: 0303 123 1113 web: www.ico.org.uk

Review

A review of the effectiveness of UK GDPR compliance and processes will be conducted by the Data Protection Officer every 24 months.

Further Information

You can exercise your right of access or find out more information about this policy by contacting the school office on 01937 843946

Disclosure of Personal Information to third parties

In general, school will only disclose personal information about individuals with their consent. However, there are circumstances under which personal information may be disclosed without consent. Some of these are listed below:

- In connection with any legal proceedings or for the purposes of the detection and prevention of crime;
- In connection with any statutory, legal duty or instruction from a Government Department to do so, such as in connection with Health and Safety legislation or the submission of the Pupil Level Annual School Census (PLASC).
- In connection with payroll and staff administration.

In any event, personal information will only be disclosed with proper justification under the DPA.

SCHEDULE 2

CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF ANY PERSONAL DATA

1 The data subject has given his consent to the processing.

2 The processing is necessary

(a) for the performance of a contract to which the data subject is a party, or

(b) for the taking of steps at the request of the data subject with a view to entering into a contract.

3 The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4 The processing is necessary in order to protect the vital interests of the data subject.

5 The processing is necessary

(a) for the administration of justice,

(aa) for the exercise of any functions of either House of Parliament,

(b) for the exercise of any functions conferred on any person by or under any enactment,

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or

(d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

6 (1)The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

(2)The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

SCHEDULE 3

CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF SENSITIVE PERSONAL DATA

1 The data subject has given his explicit consent to the processing of the personal data.

2 (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

(2) The Secretary of State may by order—

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3 The processing is necessary

(a) in order to protect the vital interests of the data subject or another person, in a case where—

(i) consent cannot be given by or on behalf of the data subject, or

(ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or

(b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4 The processing

(a) is carried out in the course of its legitimate activities by any body or association which—

(i) is not established or conducted for profit, and

(ii) exists for political, philosophical, religious or trade-union purposes,

(b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,

(c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and

(d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6. The processing

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

(b) is necessary for the purpose of obtaining legal advice, or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7. (1) The processing is necessary

(a) for the administration of justice,

(aa)for the exercise of any functions of either House of Parliament,

(b) for the exercise of any functions conferred on any person by or under an enactment, or

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

(2)The Secretary of State may by order—

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

(1)The processing

(a) is either

(i) the disclosure of sensitive personal data by a person as a member of an anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation; or

(ii) any other processing by that person or another person of sensitive personal data so disclosed; and

(b) is necessary for the purposes of preventing fraud or a particular kind of fraud.

(2) In this paragraph "an anti-fraud organisation" means any unincorporated association, body corporate or other person which enables or facilitates any sharing of information to prevent fraud or a particular kind of fraud or which has any of these functions as its purpose or one of its purposes.

8 (1)The processing is necessary for medical purposes and is undertaken by

(a)a health professional, or

(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9. (1)The processing

(a) is of sensitive personal data consisting of information as to racial or ethnic origin,

(b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and

(c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2)The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

Appendix 1

Data Protection Breach & Non Compliance Procedure

All staff and governors must be aware of what to do in the event of a DPA / UK GDPR breach. The

'Data Breach Flowchart' outlines the process.

The 'Data Breach Form' must be completed and updated as the process progresses.

Most breaches, aside from cyber criminal attacks, occur as a result of human error. They are not malicious in origin and if quickly reported are often manageable.

Everyone needs to understand that if a breach occurs it must be swiftly reported.

Examples of breaches are:-

- Information being posted to an incorrect address which results in an unintended recipient reading that information
- Loss of mobile or portable data device, unencrypted mobile phone, USB memory stick or similar
- Sending an email with personal data to the wrong person
- Dropping or leaving documents containing personal data in a public place
- Personal data being left unattended at a printer enabling unauthorised persons to read that information
- Not securing documents containing personal data (at home or work) when left unattended
- Anything that enables an unauthorised individual access to school buildings or computer systems
- Discussing personal data with someone not entitled to it, either by phone or in person. How can you be sure they are entitled to that information?
- Deliberately accessing, or attempting to access or use personal data beyond the requirements of an individual's job role e.g. for personal, commercial or political use. This action may constitute a criminal offence under the Computer Misuse Act as well as the Data Protection Act.
- Opening a malicious email attachment or clicking on a link from an external or unfamiliar source, which leads to school's equipment (and subsequently its records) being subjected to a virus or malicious attack, which results in unauthorised access to, loss, destruction or damage to personal data.

What to do?

Being open about the possible breach and explaining what has been lost or potentially accessed is an important element of working with the ICO and to mitigate the impact. Covering up a breach is never acceptable and may be a criminal, civil or disciplinary matter.

Report the breach to the Data Controller, Data Protection Compliance Manager and DPO as soon as possible, this is essential.

The breach notification form will be completed and the breach register updated.

If the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach notification to those people will be done in a co-ordinated manner with support from the DPO.

The breach report will be within 72 hours of becoming aware of the breach.

It may not be possible to investigate the breach fully within the 72 hour timeframe. Information about further investigations will be shared with the ICO with support from the DPO.

Procedure – Breach notification data controller to data subject

For every breach the school will consider notification to the data subject or subjects as part of the process. If the breach is likely to be high risk they will be notified as soon as possible and kept informed of actions and outcomes.

The breach and process will be described in clear and plain language.

If the breach affects a high volume of data subjects and personal data records, the most effective form of notification will be used and discussed with the Data Controller with support from the Data Protection Compliance Manager and DPO.

Advice will be taken from the ICO about how to manage communication with data subjects if appropriate.

A post breach action plan will be put into place and reviewed.

Evidence Collection

It may be necessary to collect information about how an information security breach or unauthorised release of data occurred. This evidence gathering process may be used as an internal process (which can include disciplinary proceedings), it may be a source of information for the ICO, it could also be used within criminal or civil proceedings.

This process will be conducted by a suitable member of school staff, which may be the Data Management Compliance Officer or Data Protection Officer, but will be determined depending on the nature of the breach.

Guidance may be required from external legal providers and police may be involved to determine the best way to secure evidence.

A record of what evidence has been gathered, stored and secured must be available as a separate log. Files and hardware must be securely stored, possibly in a designated offsite facility.

Date	Evidence Description	Secure storage location & confirmed date	School Officer

Appendix 2

Data Breach Notification Form

When did the breach occur (or become known)?	
Who was involved in the school?	
Who was this reported to?	
Date and time it was reported	
Date and time DPO notified	
A description of the nature of the breach. This must include the type of information that was lost, e.g. name, address, medical information, NI numbers	
The categories of personal data affected – electronic, hard copy	
Approximate number of data subjects affected.	
Approximate number of personal data records affected.	
Name and contact details of the Data Protection Officer / GDPR Owner.	
Consequences of the breach. What are the potential risks?	
Any measures taken to address the breach. What actions and timeline have been identified?	
Any information relating to the data breach.	