



# Sacred Heart Catholic College

---

## GDPR Policy

<b>GDPR Policy</b>	
<b>Reviewed by:</b>	Governors
<b>Approved by:</b>	Premises Health and Safeguarding
<b>Date approved:</b>	February 2021
<b>Next review due by:</b>	February 2022

# GDPR Policy

Sacred Heart Catholic College collects and uses personal information (referred to in the Data Protection Act as personal data) about staff, pupils, parents and other individuals who come into contact with the College. This information is gathered in order to enable the provision of education and other associated functions. In addition, the College may be required by law to collect, use and share certain information.

The College is registered as a Data Controller, with the Information Commissioner's Office (ICO). Details are available on the ICO website.

The College issues a Privacy Notice to all pupils/parents, this summarises the information held on pupils, why it is held and the other organisations to whom it may be passed on to.

## **Purpose**

This policy sets out how the College deals with personal information correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation.

This policy applies to all personal information however it is collected, used, recorded and stored and whether it is held on paper or electronically.

All College staff and governors involved with the collection, use, processing or disclosure of personal data will be aware of their duties and responsibilities and will adhere to this policy.

## **What is Personal Information/ data?**

Personal information or data is information which relates to a living individual who can be identified from that data, or from that data in addition to other information available to them.

Personal data includes (but is not limited to) an individual's, name, address, date of birth, photograph, bank details and other information that identifies them.

## **What is Sensitive Personal Data?**

Sensitive personal data includes information as to an individual's racial or ethnic origin, their political opinions, religious beliefs or beliefs of a similar nature, whether they are a member of a trade union, their physical or mental health or condition, sexual life, the commission or alleged commission of an offence and any proceedings for an offence committed or alleged to have been committed by them, the disposal of those proceedings or the sentence of any court in such proceedings.

## **Data Protection Principles**

The Data Protection Act 1998 establishes eight principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purpose;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subject under the Data Protection Act 1998;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

## **Commitment**

The College is committed to maintaining the above principles at all times. Therefore the College will:

- Inform individuals why personal information is being collected.
- Inform individuals when their information is shared, and why and with whom unless the Data Protection Act provides a reason not to do this.
- Obtain consent before processing Sensitive Personal Data, even if consent is implied within a relevant privacy notice, unless one of the other conditions for processing in the Data Protection Act applies.
- Check the accuracy of the information it holds and review it at regular intervals.
- Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in.
- Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Ensure that personal information is not retained longer than it is needed.
- Ensure that when information is destroyed that it is done so appropriately and securely.
- Share personal information with others only when it is legally appropriate to do so.
- Comply with the duty to respond to requests for access to personal information, known as Subject Access Requests.
- Ensure that personal information is not transferred outside the EEA without the appropriate safeguards
- Ensure all staff and governors are aware of and understand these policies and procedures.

### **Complaints**

Complaints will be dealt with in accordance with the College's complaints policy. Complaints relating to the handling of personal information may be referred to the Information Commissioner who can be contacted at Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF or at [www.ico.gov.uk](http://www.ico.gov.uk).

**Review Date: 01 February 2022**