Notre Dame
CATHOLIC SIXTH FORM COLLEGE

DATA PROTECTION POLICY

This policy adheres to and should be applied with due consideration to the College's commitment to the Framework for Ethical Leadership in Education.

Mission Statement

Our mission inspired by the Christian tradition is to be a community based on faith, hope and love; developing each individual intellectually, emotionally and spiritually to achieve their full potential.

To achieve this we will:

- Provide a welcoming, supportive community where everyone is valued.
- Provide a high quality, meaningful education which encourages the development of the whole person, inspired by the Notre Dame tradition.
- Promote a caring environment, rooted in the virtues of service, kindness, gratitude and respect.
- Work together for the benefit of each person as well as the wider community.
- Recognise, celebrate and treasure, without exception, the unique gifts and dignity of each person, ensuring equality and fairness for all, as found in the teaching and example of Our Lord Jesus Christ.

Version	3
Author	Data Protection Officer
Date Reviewed	February 2023
Approved by SLT	February 2023
Approved by Finance and Physical Resources Committee	February 2023
Review Interval	1 year
Previous review date	March 2022
Policy to be reviewed by or before	February 2024

Purpose
This policy explains the way in which the College will comply with the General Data Protection Regulation (GDPR) as it applies in the UK, tailored by the Data Protection Act 2018.

It explains the approach taken by the College to each of the data protection principles, rights and obligations. Where relevant, this policy also indicates links to related policies and procedures and the mechanisms through which compliance is planned, executed, measured and reported.

The Regulation and Act became effective in the UK on 25th May 2018.

The College is registered with the ICO reference no Z6501370.

Scope
This policy applies to all personal and sensitive personal data collected and processed by the College in whatever form.

Personal data is information that relates to an identified or identifiable individual who can be directly or indirectly identified by reference to an identifier. This can include, names, Student references, UCI's or UPN.

Sensitive Personal Data is classed as data revealing Ethnicity, Religion, Health records, sexual orientation.

This policy applies to all staff, students, governors, committee members, volunteers and third-party contractors in the handling of personal information collected by the College. The policy also applies where the College is a joint data controller or where relevant, acts as a processor for another controller

The Data Protection Principles
The GDPR and Data Protection Act 2018 contain seven Principles relating to the collection and processing of personal information. These principles are set out in the following table:

Ref	Data Protection Principle
1	Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met *('lawfulness, fairness and transparency'). Article 5(1) a*
2	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 *('purpose limitation') Article 5(1) b*
3	Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed *('data minimisation') Article 5(1) c*
4	Shall be accurate and where necessary, kept up to date *('accuracy') Article 5(1) d*
5	Shall not be kept for longer than is necessary for that purpose or those purposes *('storage limitation') Article 5(1) e*
6	Shall be kept secure i.e. protected by an appropriate degree of security *('integrity and confidentiality') Article 5(1) f*
7	Organisations shall not only adhere to the principles set out in the GDPR, but also demonstrate compliance *(Accountability) Article 5(2)*

Responsibilities

Director Of Finance and Resources

The overall responsibility for the efficient administration of the Data Protection legislation lies with the Finance Director. The Finance Director is also the Senior Information Risk Officer (SIRO) - the strategic lead for information governance and compliance with data protection legislation.

Data Protection Officer

The College is a Public Authority and must therefore appoint a Data Protection Officer under the regulation, with special responsibilities:

The DPO will work independently, report to the highest management level and will have adequate resources to enable the College to meet its GDPR obligations.

As a minimum the DPO will:

- inform and advise the College and its employees about their obligations to comply with the GDPR and other data protection laws.
- monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct periodic audits of GDPR activity and record keeping.
- be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

Lawful basis for processing

Article 6 of the GDPR, at least one of these basis's must apply whenever personal or sensitive data is processed:

1) Consent- individual has given clear consent for process for a specific purpose (Applications)
2) Contract – it is necessary to process the data before entering into a contract (Employment)
3) Legal Obligation – it is a legal requirement (DBS)
4) Vital Interests – necessary to protect a life
5) Public task – necessary to perform a task in the public interest as the official function.
6) Legitimate interests – Legitimate interests or that of a 3rd party.

When processing Special category data, as set out in Article 9, as well as one of the lawful basis as identified, there MUST a condition from the following list applies:

a) **the data subject has given explicit consent** to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject.
b) processing is necessary for the purposes of **carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law** in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.
c) **processing is necessary to protect the vital interests of the data subject or of another natural person** where the data subject is physically or legally incapable of giving consent.
d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.
e) processing relates to personal data which are manifestly made public by the data subject.

f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

g) **processing is necessary for reasons of substantial public interest,** on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

h) processing is necessary for the **purposes of preventive or occupational medicine**, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.

i) processing is necessary for **reasons of public interest in the area of public health**, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

j) processing is necessary for **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes** in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

As a college with the responsibility of education, the majority of the data that is collected and processed is done so under the principle of Public Task The College has established the lawful basis upon which it collects and processes personal information and this is held on the Data Register.

Data subject rights

The GDPR and Data Protection Act 2018 describe the rights of data subjects. The College will handle personal information in a fair and lawful manner and ensure that the exercise of each individual right is governed by a specific process as set out in the
College's records management procedures as set out in the table below:

Ref	Data Subject Right	Related Policies and Procedures
1	Right to be informed *(Articles 13 & 14)*	Privacy Notices
2	Right of access *(Article 15)*	Subject Access Request
3	Right to rectification *(Article 16)*	Subject Access Request
4	Right to erasure *(Article 17)*	Subject Access Request
5	Right to restrict processing *(Article 18)*	Subject Access Request
6	Right to data portability *(Article 20)*	Subject Access Request
7	Right to object *(Article 21)*	Subject Access Request
8	Rights related to automated decision making including profiling *(Article 22)*	Subject Access Request

Requesting access to your personal data
Under data protection legislation students have the right to request access to information about them that we hold. To make a request for this, please contact the College Data Protection Officer who will consider and process the request.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed
- claim compensation for damages caused by a breach of the Data Protection regulations
- make a subject data access request (please see link on website)

All employees have a responsibility for ensuring that any data subject access requests are passed to the DPO without delay. Subject Access Requests should be completed within 1 month of the request

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance.

If you would like to discuss, or require clarification regarding this privacy notice, please contact:

Data Protection Officer: Lisa Catherall. L.Catherall@notredamecoll.ac.uk

Data Sharing
The College will legitimately share data, as noted in the Privacy Notices, in order to provide effective services, fulfil its statutory obligations or for the purposes of crime prevention or detection and will ensure that only the minimum, relevant information is shared.

Data Protection Impact Assessment
The College recognises that the processing of personal data poses a potential risk to the "rights and freedoms" of data subjects whose information it collects and processes.

Therefore, the college will complete a DPIA to consider data breach risks on any new project or process at the beginning of the planning stage.
This should be a consideration when choosing any new supplier who will act as a data processor, or provide you with tools to allow you to process data yourselves

Personal data breaches
Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security.

Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative noncompliance, and/or financial costs.

Anyone becoming aware of a potential data breach must report it to the College DPO immediately.

This policy applies to all staff and students at the College. This includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of the College.

Types of Breach

An incident in the context of this policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the College's information assets and / or reputation. Data security breaches include both confirmed and suspected incidents.

An incident may include but is not restricted to, the following:

- loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad / tablet device, or paper record)
- equipment theft or failure
- unauthorised use of, access to or modification of data or information systems
- Attempts to gain unauthorised access to information or IT system(s)
- Unauthorised disclosure of sensitive / confidential data
- Website defacement
- Hacking attack
- Unforeseen circumstances such as a fire or flood
- Human error
- Offences where information is obtained by deceiving the organisation who holds it.

Notification

The DPO, in consultation with the Director of Finance and [where appropriate] other colleagues including [but not limited to] the IT Manager will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible.

Every incident will be assessed on a case by case basis; however, the following will need to be considered:

- Whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under Data Protection legislation
- Whether notification would assist the individual(s) affected (e.g. could they act on the information to mitigate risks?)
- Whether notification would help prevent the unauthorised or unlawful use of personal data
- Whether there are any legal / contractual notification requirements
- The dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay. Notification will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact the College for further information or to ask questions on what has occurred

The DPO must consider notifying third parties such as the police, insurers, banks or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

The DPO will consider whether the Marketing Team should be informed regarding a press release and to be ready to handle any incoming press enquiries.

A record will be kept of any personal data breach, regardless of whether notification was required.

Evaluation

Once the initial incident is contained, the DPO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

Children's Data

The College recognises that children merit special protection with regard to their personal data, as they may be less aware of how the processing may affect them and how to protect themselves and exercise their rights particularly in relation to marketing and profiling.

The College however, does not process data relating to children under the age of 13 [students at the College will generally apply for admission to College in the academic year following their sixteenth birthday] so in most cases is able to rely on the consent of the child data subject as the lawful basis for the processing of their personal data.

International Data Transfers

Transfers of Personal Data to Third Countries All exports of data from within the European Economic Area (EEA) to non-EEA countries (referred to in the GDPR as 'third countries') are unlawful unless one or more of the safeguards specified in the GDPR applies. The College ensures compliance with these requirements through the Transfers of Personal Data to Third Countries or international Organisations Procedure.

Policy review

This policy is reviewed by the Data Protection Officer (DPO) on an annual basis to ensure that:

- Its approach to privacy is fully aligned with the strategic direction of the College , its stakeholder expectations and the regulatory environment;
- That the resources required to operate the GDPR control framework effectively are available;
- The approach to data protection and the GDPR is fully integrated into the College 's business processes in particular in relation to risk and performance management;
- The objectives of the GDPR control framework are being achieved and that data protection is a key element in continuous improvement;
- The importance of compliance with data protection requirements and best practice is communicated appropriately and understood across the College.

Governance

The following table identifies who within Notre Dame Catholic Sixth Form College ("the College") is Accountable, Responsible, Informed or Consulted with regards to this policy.

The following definitions apply:

- Responsible – the person(s) responsible for developing and implementing the policy.
- Accountable – the person who has ultimate accountability and authority for the policy.
- Consulted – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- Informed – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Data Protection Officer
Accountable	Senior Information Risk Officer /Director of Finance
Consulted	Senior Leadership Team including Principal Justine Barlow, HR, ICT, Careers, Examinations office, MIS, Marketing, H&S, Finance.
Informed	The College employees, all Interim and Temporary Staff.

Corresponding Documentation

Privacy Notice for Applicants
*Please note: If the applicant's previous school contact Notre Dame Catholic Sixth Form College requesting an application status, Notre Dame Catholic Sixth Form College will share application status information in

Privacy Notice for Enrolled Students

Student Code of Conduct

Information Technology – Policy Statement

Information Security Policy

IT Acceptable use for Students

IT Acceptable use for Staff

IT Business continuity Plan

Child Protection and Safeguarding Policy and Procedures

Register of Data