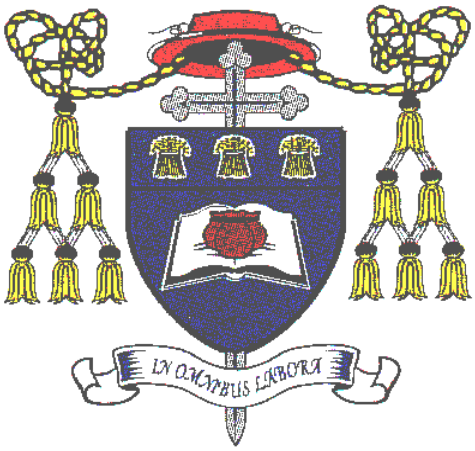

St Nicholas Catholic High School

Data Protection Policy 2021

Version Control

Current version	Previous version	Summary of changes made
2021	2021	Updated in line with guidance from DPO, Impero including; - Additional paragraph under 1.3 outlining what the policy does - Removal of Sections 8 to 14 and replace with new section 8 to simplify matters - Section 11 updated in line with DPO guidance - Section 13 – renamed 'Sharing personal data' and updated - Addition of Section 14 regarding SAR - Addition of Section 15 regarding CCTV - Addition of Section 17

Policy Impact Statement	
Policy:	
This Policy has been implemented:	
Fully	
Partially	
Occasionally	
Not at all (give reasons why)	
What revisions need to be made:	
To the Policy?	See Version Control Above

To its implementation?	

1. Legal framework

1.1. This policy has due regard to legislation, including, but not limited to the following:

- The retained EU law version of the General Data Protection Regulation (EU) (2016/17) (UK GDPR)
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

1.2. This policy will also have regard to the following guidance, among others:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
- All Article 29/European Data Protection Board Working Party Guidance on the implementation of GDPR
- Department of Education 'Data Protection: a toolkit for schools'
- IRMS Information Management Toolkit for Schools.

1.3. This policy will be implemented in conjunction with the following other school policies:

- *Records Management and Retention Policy*
- *IT Acceptable Use Policy*
- *Privacy Notices*

This Data Protection Policy sets out how St Nicholas Catholic School ("we", "our", "us") handle the Personal Data of our students, staff, parents, carers, guardians, and other third parties. This Data Protection Policy applies to the Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present students, staff, parents, carers, guardians or related third parties or any other Data Subject.
This Data Protection Policy applies to all members of staff ("you"). Members of staff must read, understand and comply with this Data Protection Policy when Processing Personal Data on our behalf.]

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Company is exposed to potential fines of up to £17.5 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the UK GDPR.

2. Applicable data

For the purpose of this policy:
2.1. Personal Data refers to information that relates a Data Subject that we can identify (directly or indirectly) from that information alone, or in combination with other identifiers we possess or can reasonably access. This includes an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data includes special categories of personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

2.2. Sensitive personal data is defined in the GDPR as 'special categories of personal data', which includes the processing of Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning physical or mental health or data concerning a natural person's sex life or sexual orientation.

2.3 Processing Personal Data is referred to throughout the GDPR and data protection legislation. This means any use of the personal information. This includes collecting, disclosing, destroying, archiving and organising, transmitting or transferring to third parties.

2.4 Data Subject is a living, identified or identifiable individual about whom we hold Personal Data. For example, the children named on a class register at a school are all Data Subjects of that register.

2.5 Data Controller is usually an organisation who dictates the reason and purpose for how data is processed. The School itself is a Data Controller as it chooses how it collects, uses and shares its own data.

2.6 The Information Commissioner's Office (ICO) is the regulator for Data Protection and Privacy law in the UK. They have the power to enforce on organisations for breaches of the Data Protection Act or the GDPR. This means they can issue: -

- An Undertaking which commits an organisation to improving their Data Protection practices.
- An Enforcement Notice ordering that an organisation does something specific e.g. train all staff to a high standard.
- A Monetary Penalty for serious and significant breaches. Under the General Data Protection Regulation this can be up to €20 Million or 4% of a company's global turnover.

2.3 This policy applies to both automated personal data and to manual filing systems.

3. Principles

3.1. We adhere to the principles relating to the Processing of Personal Data set out in the UK GDPR which require, Personal Data to be:

1. Processed fairly, lawfully and in a transparent manner (Lawfulness, Fairness and Transparency);
2. Processed for a specified, explicit and legitimate purpose (Purpose Limitation);
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);
4. Accurate and where necessary kept up to date (Accuracy);
5. Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation);
6. Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality);
7. Not transferred to another country without appropriate safeguards being in place (Transfer Limitation); and
8. Made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

3.2. The GDPR also requires that we are responsible for, and must be able to demonstrate, compliance with the data protection principles listed above (Accountability).

4. Accountability

4.1. St Nicholas Catholic High School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR. This can take a variety of forms.

4.2. Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data.

4.3. In line with best practice, we shall maintain a record of processing activities will include as a minimum the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
-

4.4. St Nicholas Catholic High School will implement measures that meet the principles of data protection, continuously creating and improving security features.

4.5. St Nicholas Catholic High School will produce Data Protection Impact Assessments where the processing of personal data is likely to result in a high risk to the

rights of the individual, where a major project requires the processing of personal data or before the introduction of new technology or a significant change to the way processing is performed.

5. **Data protection officer (DPO)**

5.1. St Nicholas Catholic High School has appointed a DPO in order to:

- Inform and advise St Nicholas Catholic High School and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor St Nicholas Catholic High School's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

5.2. The role of DPO will be carried out by an experienced and qualified member of staff as designated by Impero.

5.3. St Nicholas Catholic High School will make freely available the contact details for their appointed DPO:

Philip Crilly | Head Of Technical Support.
Direct: +44 (0) 1509 606529
Office: +44 (0) 1509 611341
Email: gdpr@imperosoftware.com

5.4. The DPO will operate independently, their role being to:

- advise the school and its employees about the obligations to comply with GDPR and other data protection requirements – this could be to assist in implementing a new CCTV system or to respond to questions or complaints about information rights.
- monitor your school's compliance with GDPR, advising on internal data protection activities such as training for staff, the need for data protection impact assessments and conducting internal audits.
- act as the first point of contact with the Information Commissioner's Office and for individuals whose data you process.

5.5. Where advice and guidance offered by the DPO is rejected by the school, this will be independently recorded.

5.6 Advice offered by the DPO will only be declined at the direction of the Head and/or Governing body and will be provided to the DPO in writing.

6. Lawful processing

6.1. The legal basis for processing data will be identified and documented prior to data being processed. The school will make it clear, at all times, the basis on which personal data is processed. The UK GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

6.2. The UK GDPR allows Processing for specific purposes, some of which are set out below. St Nicholas Catholic High School will ensure that, where it processes Personal Data it will be lawfully processed under one of the following conditions:

- Consent
- Compliance with a legal obligation.
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- For the performance of a contract with the Data Subject or to take steps to enter into a contract.
- Protecting the vital interests of a Data Subject or another person.
- For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the Data Subject.

6.3. In addition, St Nicholas Catholic High School will ensure that the processing of sensitive data will only be processed under the following conditions:

- Explicit consent of the Data Subject, unless reliance on consent is prohibited by law.
- Carrying out obligations under employment, social security or social protection law, or a collective agreement.
- Protecting the vital interests of a Data Subject or another individual where the Data Subject is physically or legally incapable of giving consent.
- Processing relates to Personal Data manifestly made public by the Data Subject.
- Processing is necessary for the establishment, exercise or defence of legal claims
- Processing is necessary for reasons of substantial public interest, on the basis of the law, with full regard for the rights and interests of the Data Subject.
- Processing is necessary for the purposes of preventive or occupational medicine, for example, the assessment of the working capacity of an employee.
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

7. Consent

7.1. Where there is no other legal basis for the processing of data St Nicholas Catholic High School may rely on the consent of individuals, both parents and pupils, in seeking consent.

7.1. Where used, consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

7.2. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

7.3. Where consent is given, a record will be kept documenting how and when consent was given.

7.4. Consent can be withdrawn by the individual at any time.

7.5. The consent of parents will be sought prior to the processing of a child's data under the age of 12 except where the processing is related to preventative or counselling services offered directly to a child.

7.6 When processing special category data or data on criminal convictions, the school will usually rely on a legal basis for processing other than consent if possible. Where explicit consent is relied on, the school must issue a Privacy Notice to the Data Subject to capture explicit consent.

8. **Data Subject's rights and requests**

8.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:
(a)withdraw Consent to Processing at any time;
(b)receive certain information about the Controller's Processing activities;
(c)request access to their Personal Data that we hold;
(d)prevent our use of their Personal Data for direct marketing purposes;
(e)ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
(f)restrict Processing in specific circumstances;
(g)challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
(h)request a copy of an agreement under which Personal Data is transferred outside of the UK;
(i)object to decisions based solely on Automated Processing, including profiling (ADM);
(j)prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
(k)be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
(l)make a complaint to the supervisory authority;
(m)in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format;

8.2 The school must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).
8.3 If a member of staff receives a request, they must immediately forward this to the school's Data Protection Lead, Vicky Hill.

9. Privacy by design and Data Protection Impact Assessments

9.1. St Nicholas Catholic High School will act in accordance with the UK GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into its processing activities.
9.2. Data Protection Impact Assessments (DPIAs) will be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy.

9.3. DPIAs will allow the school to identify data protection risks and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur.
9.4. A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.
9.5. A DPIA may be used for more than one project, where necessary and where the aims and conditions of the project are the same.
9.6. St Nicholas Catholic High School will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

9.7. Where a DPIA indicates high risk data processing, the school will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

10. Data Processors
10.1 St Nicholas Catholic High School will ensure that whenever it employs or utilises a Data Processor a written contract will be in place. The UK GDPR defines a processor as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Processors act on behalf of the relevant controller and under their authority.
10.2. Any contract will include, as a minimum, specific terms under which processing is allowed and will document:

- only act on the written instructions of the controller;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the controller and under a written contract;
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract; and
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

10.3. Where appropriate, and if and when supplied by the Information Commissioner's Office, standard clauses may be supplemented.
10.4. Any contract will clearly identify the responsibilities and liabilities of data processors in relation to:

- not to use a sub-processor without the prior written authorisation of the data controller;

- to co-operate with supervisory authorities (such as the ICO);
- to ensure the security of its processing;
- to keep records of processing activities;
- to notify any personal data breaches to the data controller;
- to employ a data protection officer; and
- to appoint (in writing) a representative within the European Union if needed.

10.5. Where a processor fails in these obligations or acts outside of the direct instructions of the school, appropriate action will be taken.

11. Data breaches

17.1. A Personal Data breach can be defined as any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

17.2. The UK GDPR requires Controllers to notify any Personal Data Breach to the Information Commissioner and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

17.3. If you know or suspect that a Personal Data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DP lead for school, Vicky Hill or alternatively , if this is not possible, the School Business Manager. You should preserve all evidence relating to the Personal Data Breach.

12. Data security

12.1. Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

12.2. Confidential paper records will not be left unattended or in clear view anywhere with general access.

12.3. 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.

12.4. 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.

12.5. All electronic devices are password-protected to protect the information on the device in case of theft.

12.6. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

12.7. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

12.8. 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.

12.9. 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.

12.10. 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.
12.11. The physical security of the school's buildings and storage systems, and access to them, is reviewed on an annual basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.
12.12. Any unauthorised disclosure or personal or sensitive information may result in disciplinary action.

13. Sharing Personal Data

13.1 Staff members may only share the Personal Data the school holds with another employee if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.
You may only share the Personal Data we hold with third parties, such as our service providers, if;
(a)they have a need to know the information for the purposes of providing the contracted services;
(b)sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
(c)the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
(d)the transfer complies with any applicable cross-border transfer restrictions; and
(e)a fully executed written contract that contains UK GDPR-approved third party clauses has been obtained.
13.2. St Nicholas Catholic High School will not publish any personal information, including photos, on its website, in social media or in any promotional or marketing publication without the permission of the affected individual or those with parental responsibility.
13.3. When uploading information to the school website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

14. Subject Access Request (SAR)

14.1 Under the Data Protection Act 1998 and GDPR May 2018, Data Subjects have a right to request access to information the school holds about them. This is known as a subject access request. Subject Access Requests can be submitted in writing, either by letter or email. Requests should include:

- The 'Subjects' name
- A correspondence address
- A contact number and email address
- Details about the information requested

The school will not reveal the following information in response to subject access requests:

- Information that might cause serious harm to the physical or mental health of the pupil or another individual
- Information that would reveal that the child is at risk of abuse, where disclosure of that

information would not be in the child's best interests
- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child

14.2 Subject access requests for all or part of the pupil's educational record will be provided within 30 calendar days and up two months if requests are excessive. No charge can be made but requests can be denied if the SAR is thought to be excessive.
14.3 Persons requesting a SAR will require evidence of their ID. Persons requesting a SAR through a third party will require written approval from the 'Subject'. Children below the age of 13 do not have the right to make a subject access request so requests must be made by parents.

15. CCTV
15.1 CCTV is used to support the safety and security of school users. We adhere to the ICO's code of practice for its use. Although consent is not required for its use prominent notices inform school users that CCTV is used within the school site.

16. Data retention
16.1. Data will not be kept for longer than is necessary in line with the schools Record Management Policy.
16.2. Unrequired data will be deleted as soon as practicable.
16.3. Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.
16.4. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

17. DBS data
17.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.
17.2. Data provided by the DBS will never be duplicated.
17.3. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

18. Changes to this policy
18.1. The school will keep this Data Protection Policy under regular review
18.2. This Data Protection Policy does not override any applicable national data privacy laws and regulations.

Reviewed by: Student Welfare & Progress Committee	Date: 26th May 2021
To be ratified by Governing Body	Date:
Review of Policy Due By	Date: May 2022
