ST. ANNE'S CATHOLIC HIGH SCHOOL FOR GIRLS

Data Protection Policy

(in accordance with the Data Protection Act 2018 and the General Data Protection Regulation – GDPR)

Autumn term 2018

Next Review: As advised by the Data Protection Officer

Resources and Personnel Committee

Mission Statement

St. Anne's Catholic High School for Girls will offer a positive presence in Enfield with a comprehensive curriculum, equipping students with the ability to meet the challenges of the 21st Century confidently and with high spiritual and moral standards.

We recognise that students, parents, staff and governors make up the school's community which will continually self-evaluate to improve itself effectively and efficiently in all aspects of its growth.

We are a fully inclusive, Catholic girl's secondary school meeting high academic standards, promoting spirituality, pastoral care and the Catholic community.

We recognise in all our relationships the dignity and value of each person showing one another mutual acceptance and respect.

'Act justly, love tenderly, walk humbly with your God.'

CONTENTS

1. Introduction

1.1 St. Anne's Catholic High School for Girls is required, as part of its overall information governance structure, to ensure that appropriate controls are implemented and maintained in relation to the collection, use and retention of personal information pertaining to its pupils, parents, schools workforce and contractors; and that these are in accordance with the requirements of the current data protection law as enacted. (The Data Protection Act 2018 (DPA) and the Applied General Data Protection Regulation (GDPR))

1.2 This document provides a framework for our School workforce to meet legal and corporate requirements in relation to information requests that fall within the scope of the legislation.

1.3 The Policy applies to all personal information created, received, stored, used and disposed of by the School irrespective of where or how it is held.

1.4 It must be noted that compliance is a **legal** requirement and that individuals can face prosecution for breaches of its Principles.

2 Aim of the Policy

2.1 The aim of this document is to clarify the School's legal obligations and requirements for the processing of personal data and to ensure that all such data is:

- collected, stored and processed for justifiable school business reasons
- has appropriate legal basis or informed consent for use, and is not combined with other data or used for other purposes without appropriate legal basis or consent
- used only by those persons with a legitimate reason for access
- stored safely
- retained only for the defined time period
- not disclosed to unauthorised persons, and transfers to authorised persons recorded

2.2 St. Anne's Catholic High School for Girls will actively seek to meet its obligations and duties in accordance with the law and in so doing will not infringe the rights of its employees, customers, third parties or others.

3 Scope

3.1 The scope of this policy requires compliance with the principles defined in law.

Personal Data is defined as: personal data relating to an identifiable living individual and includes the expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information as to:

- racial or ethnic origin
- political opinions
- religious or other beliefs
- trade union membership
- physical or mental health or condition
- sexual life
- commission of criminal offences or alleged offences.

3.2 Sensitive personal data may only be stored or processed for a limited variety of purposes. All processing of sensitive personal data without a legal basis for use must be cleared by the Information Commissioner.

3.3 All personal data must be protected, and sensitive personal data may require special protection measures.

3.4 Changes to use or new uses of personal data require consultation with the Data Protection Officer (DPO). Their advice must be recorded and if dissented from, the dissent and alternate action taken recorded.

4 Data Protection Principles

4.1 The GDPR includes principles, as does the DPA, which must be adhered to whenever personal data is processed. Processing includes obtaining, recording, using, holding, disclosing and deleting personal data.

4.2 All personnel processing personal information in the course of their business functionality must ensure they adhere to the principles in the GDPR Article 5 (the DPA eight principles cover similar ground, but the GDPR is more developed) which require that:

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject **('lawfulness, fairness and transparency');**

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes **('purpose limitation');**

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed **('data minimisation');**

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay **('accuracy');**

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject **('storage limitation').** Note that there are additional requirements on location of storage and processing elsewhere in the laws**;**

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('**integrity and confidentiality').**

2.The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 **('accountability').**

Further information on the principles can be found on the Information Commissioner's Office website.

5 The Information Commissioner's Office

5.1 The Information Commissioner (ICO) administers Data Protection in the UK. The role and duties of the Commissioner include:

- ensuring compliance with the law
- ensuring that individuals rights to privacy are respected
- ensuring that individuals have access to data held about themselves
- establishing and maintaining a Register of data users and making it publicly available
- investigating complaints, serving notices on registered data users who are contravening the principles of the Act, and where appropriate prosecute offenders.

5.2 The law gives the Information Commissioner wide powers to ensure compliance, including warrants to search and seize documents and equipment.

6 Access and Use of Personal Data

6.1 This policy applies to everyone that has access to personal data, and includes any third party or individual who conducts work on behalf of School or who has access to personal data for which School is responsible and who will be required contractually or otherwise to comply with this policy.

6.2 Deliberate unauthorised access to, copying, disclosure, destruction or alteration of or interference with any computer equipment or data is strictly forbidden and may constitute a criminal and/or a disciplinary offence.

6.3 It is an offence for any person to knowingly or recklessly obtain, procure or disclose personal data, without the permission of the data controller (School) subject to certain exceptions.

6.4 It is also an offence for someone to sell or offer to sell personal data.

6.5 All data subjects are entitled to:

- Know what information School holds and processes about them and why it is held
- Know who can gain access to it, who it is shared with and where it is stored
- How to keep this data up-to-date
- Know what action School takes to comply with its obligations

6.6 All data subjects may request erasure of data which they feel is no longer relevant.

6.7 This School will ensure that compliance with this Policy is monitored and the School is able to evidence that it is complying with its legal responsibilities.

7 School Commitment

7.1 To achieve the overall aim of the Data Protection Policy the School will:

- Provide adequate resources to support an effective corporate approach to Data Protection.
- Respect the confidentiality of all personal information irrespective of source.
- Publicise the School's commitment to Data Protection.
- Compile and maintain appropriate procedures and codes of practice.
- Promote general awareness and provide specific training, advice and guidance to its workforce at all levels and.
- Monitor and review compliance with legislation and introduce changes to policies and procedures where necessary.

8 Roles and Responsibilities

8.1 The **Data Subjects** are those natural persons about whom the school retains information.

8.2 Ultimate accountability for all decisions made relating to Data Protection lies with the **Governing Body**.

8.3 The **Governing Body** is responsible for ensuring that sufficient resources are provided to support the requirements of this policy as well as making strategic level decisions which impact on how School carries out its obligations under the legislation. The School Business Manager (SBM) is responsible for monitoring compliance within the school setting and taking any necessary corrective action.

8.4 The **Governing Body** monitors, oversees, reports and makes recommendations to the Head Teacher and School Business Manager on all strategic level DPA issues.

8.5 The School Business Manager has the role of handling requests for data (SARs, FOIs, EPAs etc.) and complaints about the school's use of data. The School Business Manager will also maintain and provide reporting to Governing Body on these issues.

8.6 The **Data Protection Officer** (DPO) will provide advice and guidance in conjunction with Legal Services on legal compliance and best practice. Advice of the DPO must be sought for all new or changed data uses; this advice must be formally recorded and if not followed, this fact must also be recorded. The DPO acts as the liaison between the ICO and the School. The DPO also acts as independent reviewer/advisor on complaints and provides a lead for raising awareness of Data Protection issues.

8.7 **Dataset Owners** are the central contact to compliance. Dataset Owners will also help the School Business Manager process requests and have a responsibility to ensure that data stored on systems is captured, stored, processed, accessed and deleted in line with the law and the School's Retention schedule. They are additionally responsible for ensuring that the recording of all statutory requirements are kept up to date, and reviewed at least annually.

8.8 The **School Business Manager** is directly responsible for compliance with the Act within the school and ensuring adherence by their staff.

8.9 **All School employees** and personnel working with personal data have a responsibility to ensure that they have sufficient awareness of the data protection law so that they are able to comply with the requirements of the law.

9 Responsibilities of School's Workforce

9.1 The processing of personal data is to be compliant with legal, industry, regulatory and business requirements; it is the responsibility of school workforce to

be aware of and conversant with these requirements for the processing and management of personal data in an appropriate manner.

9.2 Some data supplied by others will have handling requirements beyond the School's normal criteria. Staff involved must be made aware of this by the School Business Manager and are then responsible for handling it correctly.

9.3 The following minimum requirements are applied to everyone who comes into contact with personal data:

- The School workforce is to ensure that personal data is to be processed accurately
- When not required for immediate use personal data is to be secured from unauthorised viewing and access
- Personal data must not be sent to/from personal (non-work) email accounts
- Personal information can only be distributed externally if it is:
    - Being sent to someone with an appropriate data sharing or processing agreement with the school, a legal right to access and a need to know
    - sent via Egress encrypted e-mail or otherwise securely distributed as agreed with the DPO.
- Computer systems that process, access or store such data are to have password protected screen savers activated when left unattended, and all data should be encrypted at rest.
- The carrying of personal, sensitive or confidential information outside school environments should be avoided wherever possible. If this is unavoidable, then encryption of the device and device management by School is recommended. Paper based documents holding personal or sensitive information must be concealed from public view in transit and held securely when stored.
- When no longer required to be retained all personal data is to be disposed of securely, i.e. by shredding or via secure waste disposal.
- Personal data may not be stored on removable media devices without explicit management approval and appropriate encryption controls. Such data is to be removed from the removable media as soon as practically possible.
- The discussion of personal data with unauthorised persons either inside or outside the School is expressly prohibited. This also includes, but is not limited to, email, social networking sites, blogs, forums, instant messaging services, chat rooms etc.
- Staff are required to complete the Data Privacy and Information Security training on joining the organisation and as required thereafter.

10 Data Controller

10.1 In accordance with the DPA, School as a corporate body is the Data Controller and is therefore ultimately responsible, through the appointed Data Protection Officer or the person fulfilling that role, for the implementation of this policy.

10.2 The School will also appoint designated Data Owners who are responsible for the day-to-day management of the data within their business areas of responsibility to ensure that compliance with law and documentation of personal data use is maintained.

11 Data Protection Officer

11.1 The DPO is responsible for fulfilling the role as documented in the data protection law.

11.2 The DPO must be involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

11.3 The DPO is invited to participate regularly in meetings of senior and middle management. His or her presence is recommended where decisions with data protection implications are taken. All relevant information must be passed on to the DPO in a timely manner in order to allow him or her to provide adequate advice.

11.4 The opinion of the DPO must always be given due weight. In case of disagreement, the reasons for not following the DPO's advice must be recorded and formally communicated.

11.5 The DPO must be promptly consulted once a data breach or another incident has occurred.

11.6 The DPO will keep the SBM informed of data protection issues pertaining to the School, including any changes in legislation that might impact business processes.

11.7 The DPO will ensure that Data Privacy and Information Security training is available to staff and that a record of completion is maintained.

12 Dataset Owner

12.1 Dataset Owners will work to facilitate the daily activities and management responsibilities under the law.

12.2 Dataset Owners must inform the DPO of any proposed new or changed uses of personal information within their business unit before any change in process or additional information collection is authorised.

12.3 Dataset Owners must regularly review the content and use(s) of personal information, and confirm to the DPO that the information held is complaint with current law.

12.4 Dataset Owners must ensure that members of school workforce and contractors are conversant with their responsibilities under the law, and that they know the procedures to follow when handling, releasing and disposing of information.

12.5 Dataset Owners (along with the School Business Manager) are responsible to ensure that SARs and other requests for information are processed within the required time limits.

12.6 Dataset Owners will assist the DPO with the collation of materials in response to any access request or complaint received.

13 Training and Awareness

13.1 **All the School workforce** has a responsibility to ensure that they and the staff they manage have undertaken the Data Privacy and Information Security training and have sufficient awareness of the law so that they are able to comply with the requirements.

13.2 It is mandatory that all School workforce that have access to personal data or to the network to undertake the Data Privacy and Information Security training. New entrants will be expected to undertake and successfully complete the module as part of the induction process. Established staff will be expected to undertake and complete refresher training as directed.

13.3 Managers should encourage and make time for their staff to attend any further Data Privacy and Information Security training or awareness opportunities that may arise.

13.4 Failure to complete the courses within the prescribed period could result in disciplinary action proceedings.

14 Collection of Data

14.1 The School collects and records personal data from various sources, including that obtained or provided by the data subjects themselves.

14.2 In some instances, data may be collected indirectly through monitoring devices, including but not limited to: door access control systems, CCTV, personal

recording devices and physical security logs or electronic monitoring systems. For further detail refer to School's Information Security Policy.

15 Accuracy and Relevance

15.1 It is the responsibility of those who receive personal information to ensure so far as possible, that it is accurate and up to date. Personal information should be checked at regular intervals, to ensure that it is still accurate.

15.2 If the information is found to be inaccurate, steps must be taken to rectify it. Individuals who input or update information must also ensure that it is adequate, relevant, unambiguous and professionally worded. Data subjects have a right to access personal data held about them and have inaccuracies corrected.

16 Rights to Access, Correct and Remove Information

16.1 Data subjects have the right to access any personal information (data) about them that is held.

16.2 Data subjects also have the right to have data about themselves corrected or erased subject to certain conditions.

16.3 The School aims to comply with requests as quickly as possible but will ensure that it is provided within one calendar month unless there is a good reason for any delay. In such cases the reason for a delay will be explained in writing to the person making the request.

17 Fair and Lawful Processing

17.1 When the School processes personal data, it must have a legal basis for doing so or a freely given, positive consent. The law provides a list of conditions to ensure that personal information is processed fairly and lawfully:

- Personal information is only processed where it is justified, and this is transparent to the data subject.
- Information on the processing is easily accessible and easy to understand, in clear and plain language.
- That data subjects are aware of risks, rules, safeguards and rights in respect of processing and how to exercise their rights.
- That the minimum amount of personal data is kept, and for as short a period as possible.

- That sensitive personal information is processed only where necessary and justified, and with permission for this from the ICO unless a legal basis for processing is used.

17.2 Individuals that supply the School with personal information are provided with a 'Privacy Notice' (or online privacy statement) at time of data collection, repeated at time of SAR, which communicates the following:

- Purposes, categories, recipients (esp. outside country)
- Period of storage
- Existence of the right to request rectification, erasure and to object to processing
- Right to complain to supervisory authority and contact
- Information on communication and source
- Information on significance and consequences of processing

18 Data Sharing

18.1 Where School shares personal information with any third party a 'Data Sharing Agreement' or 'Data Processing Agreement' must exist as part of a formally documented written agreement or contract.

18.2 A 'Data Sharing Agreement' is required if the information supplied is being used to fulfil requirements of the recipient.

18.3 A 'Data Processing Agreement' is required if the information supplied is being used only to fulfil School requirements and not used otherwise by the recipient.

18.4 Where the other party uses the personal information for its own purposes (Data Sharing):

- The agreement or contract will clearly describe the purposes for which the information may be used and any limitations or restrictions on the use of that information
- The other party is to provide an undertaking or provide other evidence of its commitment to process the information in a manner that will not contravene the law

18.5 Where the processing of personal information with a third party is required by law, procedures are to ensure that the protocols and controls for the sharing of the data are documented, regularly reviewed and verified.

18.6 Requests for personal information from the Police or other enforcement agencies can be considered where the purpose is for the prevention or detection of a crime and or the collection of taxes. It should be noted however that the School is under no obligation to do so. Before providing the information, the requesting agency must provide a sufficient explanation of why the information is necessary to the extent that not providing it may prejudice an investigation. This is to satisfy the

relevant information holder that the disclosure is necessary. The request must be on letter headed paper and authorised by a senior officer from the requesting agency (Police Inspector or equivalent). If the information is to be disclosed, the disclosure must be authorised by the SBM (or above) and a note for the record should be made of the details about the disclosure with an explanation of why the disclosure is appropriate.

19 Data Retention and Disposal

19.1 School must ensure that personal information is not kept for any longer than is necessary; this is to adhere to any legal, regulatory or specific business justification.

19.2 School will retain some forms of information longer than others, but all decisions are to be based upon business requirements; details can be found in the Record Retention Schedule.

19.3 Data relating to clients is only to be retained for as long as a business justification remains.

19.4 When disposing of information, equipment or media, the School's confidential waste disposal policy and procedures should be adhered to.

19.5 The retention criteria must be imposed on third parties with who data is shared.

20 Transfer Outside of the European Economic Area (EEA)

20.1 To ensure an adequate level of protection is applied to personal information transferred or processed outside the EEA contracts are to include conditions relating to the specific requirements for the protection of the information.

20.2 School is responsible for ensuring that 'due diligence' is conducted on the other party, and that adequate and appropriate controls and safeguards are applied for the transfer of the personal information.

20.3 Companies outside the EEA are to be required to apply the same controls and requirements as applied within the EEA unless they can demonstrate other adequate procedures are implemented to protect the personal information as part of the 'due diligence' process. Periodic reviews of the same are to be conducted to ensure adherence is maintained.

20.4 Specific issues with cloud processing should be recorded by the school and the cloud policy and procedures should be followed.

20.5 Data received by School from third parties may have specific storage and use rules that may further restrict where it can be stored or processed (e.g. Health data cannot be stored outside England & Wales).

21 Violations

21.1 Unauthorised disclosure of personal data is a disciplinary matter that may be considered a gross misconduct and could lead to termination of employment.

21.2 In the case of third parties unauthorised disclosure could lead to termination of the contractual relationship and in certain circumstances this could give rise to legal proceedings.

21.3 Any failure to follow this Policy must be treated as an incident and investigated in accordance with the Security Incident Reporting Procedure.

22 Supporting Policies

This policy should be read in conjunction with the following policies and procedures:

- Staff Acceptable Use Policy
- Subject Access Policy and Procedure
- Freedom of Information Policy
- Security Incidents Reporting Procedure
- Use of Cloud Services Security Procedures