# St Catherine's College

# GDPR – Data Protection Policy Statement

## 1 Introduction

## 1.1 Background to the General Data Protection Regulation ('GDPR')

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

## 1.2 Definitions (drawn from the GDPR)

Material scope (Article 2) – the GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

Territorial scope (Article 3) – the GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behavior of data subjects who are resident in the EU.

Members of the College – where this document states to members of the College, it is referring to students, visiting students, employees, SCR members, other academic members, alumni and supporters of the College.

Partners - where this document states to partners of the College, it is referring to suppliers and contractors.

## 1.3 Article 4 Definitions

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre.

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to 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.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data – St Catherine's College.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling **–** is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behavior. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling. St Catherine's College does not undertake any profiling activities.

Personal data breach **–** a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent **-** means 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.

Child **–**The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

## 2 Policy Statement

2.1 The Governing Body and management of St Catherine's College are committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information St Catherine's College collects and processes in accordance with the General Data Protection Regulation (GDPR).

2.2 Compliance with the GDPR is described by this policy and other relevant policies such as the College's Information Security Policy (ISP), along with connected processes and procedures.

2.3 The GDPR and this policy apply to all of St Catherine's College's personal data processing functions, including those performed on students, employees, suppliers, guest, partner and any other personal data the organisation processes from any source.

2.4 The Data Protection Officer is responsible for reviewing the College's published Registers Of Processing Activities (ROPA)at least annually in the light of any changes to St Catherine's College's activities) and to any additional requirements identified by means of data protection impact assessments.

2.5 This policy applies to all members, guests and partners of St Catherine's College such as outsourced suppliers. Any breach of the GDPR will be dealt with under St Catherine's College's disciplinary procedures and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

2.6 Partners and any third parties working with or for St Catherine's College, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by St Catherine's College without having entered into an appropriate agreement with St Catherine's College. These agrements impose on the third party obligations no less onerous than those to which St Catherine's College is committed.

## 3 Responsibilities and Roles under the GDPR

3.1 St Catherine's College is a data controller and a data processor under the GDPR.

3.2 College Officers and all those in managerial or supervisory roles throughout St Catherine's College are responsible for developing and encouraging good information handling practices within St Catherine's College.

3.3 The Data Protection Officer, who Governing Body considers to be suitably qualified and experienced, has been appointed to take ultimate responsibility for St Catherine's College's compliance with this policy. On a day-to-day basis the College IT Manager has responsibilities for ensuring that St Catherine's College complies with the GDPR operationally.

3.4 The Data Protection Officer has responsibility to ensure procedures such as Subject Access Request are responded to in a timely fashion for all members, guests and partners of the College seeking clarification on any aspect of data protection compliance.

3.5 Compliance with data protection legislation is the responsibility of all members, guests and partners of St Catherine's College who process personal data.

3.6 St Catherine's College will provide training and awareness requirements in relation to specific roles responsible for processing personal data.

3.7 Members, guests and partners of St Catherine's College are responsible for ensuring that any personal data about them and supplied by them to St Catherine's College is accurate and up-to-date.

# 4 Data Protection Principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. St Catherine's College's policies and procedures are designed to ensure compliance with the principles.

4.1 Personal data must be processed lawfully, fairly and transparently

Lawful – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example contractual.

Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

The GDPR has increased requirements about what information should be available to data subjects in the 'Transparency' requirement.

Transparency – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

St Catherine's College's Privacy Notices, Registers of Processing Activities (ROPAs) & procedures are set out online here.

These include specific information on:

4.1.1 the contact details of the Data Protection Officer;
4.1.2 the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
4.1.3 the period for which the personal data will be stored;
4.1.4 the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
4.1.5 the categories of personal data concerned;

4.1.6 the recipients or categories of recipients of the personal data, where applicable;

4.1.7 where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;

4.1.8 any further information necessary to guarantee fair processing.

4.2 Personal data can only be collected for specific, explicit and legitimate purposes

4.2.1 Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of St Catherine's College's GDPR Registers of Processing Activities (ROPA).

4.3 Personal data must be adequate, relevant and limited to what is necessary for processing

4.3.1 The Data Protection Officer is responsible for ensuring that policies are in place so St Catherine's College does not collect information that is not strictly necessary for the purpose for which it is obtained.

4.3.2 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a link to privacy statement and be approved by the Data Protection Officer or IT Manager.

4.3.3 The Data Protection Officer will ensure that, on an annual basis, all data collection methods are reviewed to ensure that collected data continues to be adequate, relevant and not excessive.

4.4 Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

4.4.1 Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

4.4.2 The Data Protection Officer is responsible for ensuring that relevant staff are trained in the importance of collecting accurate data and maintaining it.

4.4.3 It is also the responsibility of the data subject to ensure that data held by St Catherine's College is accurate and up to date.

4.4.4 Members, guests and partners of the College should be required to notify the College of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of St Catherine's College to ensure that any notification regarding change of circumstances is recorded and acted upon.

4.4.5 The Data Protection Officer and all College Officers are responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

4.4.6 On an annual basis, the Data Protection Officer, in concert with relevant managers, will review the retention dates of all the personal data processed by the College, by reference to the College's Register of Processing Activities (ROPA), and will identify

any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed.

4.4.7 The Data Protection Officer is responsible for ensuring responses and execution of requests for rectification from data subjects are completed within one month. This can be extended to a further two months for complex requests. If St Catherine's College decides not to comply with the request, the Data Protection Officer must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority.

4.4.8 The Data Protection Officer is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

4.5 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

4.5.1 Personal data will be retained in line with the Registers of Processing Activities(ROPA), once its retention date is passed, it must be securely destroyed or archived as set out in the ROPAs.

4.5.2 The Data Protection Officer must specifically approve any data retention that exceeds the retention periods defined in the ROPAs, and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

4.6 Personal data must be processed in a manner that ensures the appropriate security

4.6.1 The Data Protection Officer will ensure a clear data classification scheme exists along with data handling and storage security guidelines.

When assessing appropriate organisational measures the Data Protection Officer will consider the following:

- The appropriate training levels throughout St Catherine's College;
- Measures that consider the reliability of employees (such as references etc.);
- Confidentiality agreements with anyone accessing St Catherine's College data;
- Identification of disciplinary action measures for failing to report data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper based records;
- Adoption of a clear desk policy;
- Storing of paper based data in lockable cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employee's own personal devices being used in the workplace;
- Adopting clear rules about passwords/passphrases;

- Ensuring regular, encrypted backups of personal data and storing media across multiple sites;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

St Catherine's College's compliance with these principles is contained in its Information Security Policy.

4.7 The controller must be able to demonstrate compliance with the accountability principle

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements.

The College will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design and breach notification procedures.

# 5 Data Subjects' Rights

5.1 Data subjects have the following rights regarding data processing, and the data that is recorded about them:

5.1.1 To make subject access requests regarding the nature of information held and to whom it has been disclosed.

5.1.2 To prevent processing likely to cause damage or distress.

5.1.3 To prevent processing for purposes of direct marketing.

5.1.4 To sue for compensation if they suffer damage by any contravention of the GDPR.

5.1.5 To take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data.

5.1.6 To request the supervisory authority to assess whether any provision of the GDPR has been contravened.

5.1.7 To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.

5.1.8 To object to any automated profiling that is occurring without consent.

5.2 St Catherine's College ensures that data subjects may exercise these rights:

5.2.1 Data subjects may make subject access requests (SAR) by contacting the Data Protection Officer at St Catherine's. DPO@stcatz.ox.ac.uk

5.2.2 Data subjects have the right to complain to St Catherine's College about the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the Information Commissioners Office best practice.

# 6 Consent

6.1 St Catherine's College understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

6.2 Where consent is relied on for the keeping of data, there must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication.

6.3 In the majority of instances, consent to process personal and special category data is obtained by St Catherine's College contractually e.g. when a new student signs a student contract, or during an application process.

# 7 Security of Data

7.1 All College members, guests and partners are responsible for ensuring that any personal data that St Catherine's College holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by St Catherine's College to receive that information.

7.2 All personal data should be accessible only to those who need to use it, and access may only be granted in line with the College's Information Security Policy.

7.3 Care must be taken to ensure that PC screens and terminals are not visible except to authorised personnel. All employees (and other members) are required to enter into a confidentiality agreement before they are given access to College data.

7.4 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit written authorisation from either the Data Protection Officer. As soon as manual records are no longer required for day-to-day customer support, they must be shredded or securely archived in line with College Registers of Processing Activities(ROPAs) and data handling scheme.

7.5 Personal data may only be deleted or disposed of in line with the Registers of Processing Activities(ROPAs) and data-handling scheme. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed, secure wiped and destroyed as required by the College's Information Security Policy before disposal.

7.6 Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised by either the Data Protection Officer to process data off-site.

# 8 Disclosure of Data

8.1 St Catherine's College must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies (except where required to by law. E.g. tax information to HMRC). All College members, guests and partners of the College should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of St Catherine's College's business.

8.2 All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer.

# 9 Retention and Disposal of Data

9.1 St Catherine's College will not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

9.2 St Catherine's College may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

9.3 The retention period for each category of personal data is set out in the College's Registers of Processing Activities(ROPAs) along with the criteria used to determine this period including any statutory obligations St Catherine's College has to retain the data.

# 10 Data Transfers

10.1 All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

10.2 St Catherine's College does not export persona data to any party outside the EU.

# 11 Information Assets

11.1 St Catherine's College has established detailed Registers of Processing Activities(ROPAs), A Retention Schedule and a Data Sharing Table (available online here as part of its approach to address risks and opportunities throughout its GDPR compliance project.

These documents determine:

- business processes that use personal data;
- source of personal data;
- description of personal data;
- processing activity;

- maintains the inventory of data categories of personal data processed;
- documents the purpose(s) for which each category of personal data is used;
- recipients, and potential recipients, of the personal data;
- the role of the St Catherine's College throughout the data flow;
- any data transfers; and
- all retention periods.

11.2 St Catherine's College is aware of any risks associated with the processing of particular types of personal data.

11.2.1 St Catherine's College assesses the level of risk to individuals associated with the processing of their personal data and specifies handling processes based on the classification of that data.

11.2.2 St Catherine's College shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

11.2.3 The Data Protection Officer shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority (ICO).

The Data Protection Officer is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

Version 1.0 Published 18 May 2018