Data Protection Policy

1. Purpose and Scope

1.1 Christ the Redeemer College is committed to ensuring compliance with data protection legislation and to promoting good practice in information management.

1.2 The College seeks to make a positive difference to the individuals and communities through the contribution of our staff, students and graduates, and this includes upholding the data protection principles and facilitating the rights of data subjects. Additionally, compliance with data protection legislation shapes efficient working practices and significantly reduces the risks of an information security breach, which in turn reduces the risk of causing harm and/or distress to data subjects, reputational damage, financial damage and undertakings from the Information Commissioner's Office.

1.3 This policy applies to all individuals and organisations that process personal data on behalf of the College, including but not limited to:

- employees, consultants, contractors and temporary workers
- students performing paid or voluntary work for the College
- organisations associated with and officially recognised by the College
- third parties associated with the College, such as research collaborators.

2. Principles

2.1 Christ the Redeemer College needs to process personal data in order to deliver its core learning, teaching and research functions, operate effectively as a business and meet legislative, contractual and statutory obligations.

2.2 The personal data relates to:

- past, present and prospective students including alumni and those of collaborative partners
- past, present and prospective employees
- regulatory bodies
- suppliers
- research subjects
- supporters and others with whom it has dealings.

2.3 Under the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA 2018), the College is a data controller and must comply with data protection legislation.

3. Background

3.1 The General Data Protection Regulation (GDPR) is the EU legal framework for data protection and underpins the Data Protection Act 2018 (DPA 2018). The GDPR applies to all member states and the DPA 2018 applies to the UK, both from the 25 May 2018, replacing the UK's Data Protection Act 1998. The GDPR is designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organisations across the EU area approach data privacy.

3.2 As defined in the DPA 2018 and Article 2 of the GDPR the material scope encompasses 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.

3.3 As defined in the DPA 2018 and by Article 3 of the GDPR, the territorial scope encompasses all controllers that are established in the EU (European Union) who process the personal data of data subjects. It also applies to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behaviour of data subjects who are resident in the EU. Although the UK is no longer a member state of the European Union, the intention of this policy is to ensure that the College remains aligned with both UK and EU data protection legislation and requirements.

3.4 As explained by the Information Commissioner's Office website, 'personal data only includes information relating to natural persons who can be identified or who are identifiable, directly from the information in question; or who can be indirectly identified from that information in combination with other information. Information about a deceased person does not constitute personal data and therefore is not subject to the GDPR. Information about companies or public authorities is not personal data. However, information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable and the information relates to them as an individual may constitute personal data.' (ICO website June 2019)

4. Processing of Personal Data

4.1 Accountable, lawful processing of personal data is vital to the successful operation and reputation of the College, and for maintaining the trust of our students, employees and other stakeholders. The College is committed to protecting the rights and freedoms of individuals in accordance with the provisions of data protection legislation. In order to achieve this, the College will ensure that personal data is handled appropriately and consistently.

4.2 In accordance with the data protection principles of the GDPR and DPA 2018, Commonwealth Education Foundation will ensure that personal data is:

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- 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 not be considered to be incompatible with the initial purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date; every reasonable step shall be taken to ensure that personal data is accurate, having regard to the purposes for which it is processed, erased or rectified without delay
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data shall be stored for longer periods insofar as the personal data shall be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR and DPA 2018 in order to safeguard the rights and freedoms of individuals
- 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

4.3 Commonwealth Education Foundation, as a data controller, shall be responsible for and be able to demonstrate compliance with the principles of data protection legislation.

4.4 Where the lawful basis for processing personal data is consent, a record of the consent shall be kept for as long as the personal data is kept.

4.5 All processing of personal data by third parties on behalf of the College, where the College is data controller, shall be covered by appropriate contracts or data sharing agreements and shall include adequate data protection clauses.

5. Rights of Data Subjects

5.1 Data subjects have rights regarding data processing, and the data that is recorded about them. The College facilitates these rights as they are defined by the Information Commissioner's Office:

- The right to be informed (Article 14)
- The right of access (Article 15)
- The right to rectification (Article 16)
- The right to erasure (Article 17)
- The right to restrict processing (Article 18)
- The right to data portability (Article 20)
- The right to object (Article 21)
- Rights in relation to automated decision making and profiling (Article 23).

5.2 The College does not carry out any automated decision making or profiling, however the reference to the Article 23 rights is included in this policy in order to ensure that the College facilitates those rights should they become applicable.

5.3 The Article 14 'right to be informed' is primarily fulfilled through the timely provision of privacy notices. The College website hosts privacy notices relating to staff, students and alumni.

5.4 The Article 15 'right of access' is detailed further on the College's website and Data Subject Access Requests (DSARs) are processed by the Data Protection Lead, who liaises with staff as appropriate.

5.5 The College has procedures to facilitate the data protection principles and rights of the data subject appropriately. Staff must follow the procedures provided on the College's website and VLE and ask their Data Protection Lead if they are unsure of any procedure.

5.6 If a data subject contacts any part of the College to exercise any of their rights, the person contacted should liaise with the Data Protection Lead for advice or the data subject should be put in direct contact with the Data Protection Lead (dataprotection@christredeemer.ac.uk) who will enable them to exercise their rights.

6. Sharing of Personal Data

Implementation

6.1 Ensuring that personal data is shared appropriately is vital to the successful operation and the reputation of the College, and for maintaining the trust of our employees, students and other stakeholders. In order to achieve this, the College will:

6.1.1 Undertake a data protection impact assessment screening for any new initiatives that involve the sharing of personal data. Where sharing is likely to result in a high risk to the rights and freedoms of natural

persons (particularly where new technology is involved) a full data protection impact assessment will be completed.

6.1.2 Ensure that the sharing of personal data is necessary to achieve the identified objective(s). Anonymised or pseudonymised data will be shared where the identification of data subjects is not required.

6.1.3 Implement information classification with procedures for the secure sharing of special category data or personal data that could be considered a high risk to the rights and freedoms of individuals.

6.1.4 Share the minimum amount of personal data required to achieve the objective(s) in a practical way.

6.1.5 Provide data subjects with privacy notices and, where data subjects have a choice, seek consent for the sharing of their personal data.

6.1.6 Record all decisions to share personal data with organisations other than Commonwealth Education Foundation.

6.1.7 Ensure that a written agreement (i.e. contract or data sharing agreement) is in place with external parties where personal data is shared on a systematic basis or there is a large-scale transfer of personal data. Such agreements will, as a minimum, include:

- The classes, or specific items, of personal data to be shared
- The source(s) of the personal data
- The objective(s) of the data sharing arrangement
- The lawful basis for sharing the personal data
- The individuals/groups that will have access to the personal data
- The methods by which the personal data will be transferred, including any controls for protecting the data from loss, destruction or unauthorised access
- The frequency with which the personal data will be shared
- Storage requirements for the personal data, including any controls for protecting the data from loss, destruction or unauthorised access
- The parties' responsibilities for ensuring the accuracy of the personal data
- Retention and disposal requirements
- Arrangements for enabling data subjects to exercise their rights
- Processes and procedures for handling information security incidents.

Sharing of personal information with a student's partner / relatives

6.2 The College has a requirement to treat all students as adults and does not act in loco parentis ("in the place of a parent") in relation to students, regardless of their age. In accordance with data protection laws there are limited situations where the College shares personal information about students or discusses their circumstances. The College will only share such information with a student's partner or relatives with explicit written consent from the student, where the College is satisfied that this consent has been provided voluntarily by the student and that they have not been coerced into providing this consent.

6.3 For students under the age of 18, the College requires the contact details of a parent/guardian. Although those under 18 are regarded as children under UK law, they still have the legal right for information about them not to be disclosed without their explicit written consent as set out above. The College therefore requires all students under the age of 18 years to provide consent for the disclosure of appropriate information to their parent or guardian, upon commencing their studies. This consent will remain in force until the student's 18th birthday.

6.4 The information above does not apply to a Data Subject Access Request (DSAR). A student's partner / relative cannot submit a DSAR on behalf of a student, even with the student's written consent, unless there is reason to believe that the student does not have capacity to submit the DSAR themselves. References to

written consent may be interpreted in an appropriate way, agreed by all parties, to take account of disabilities.

7. Support of the Data Protection Lead

7.1 The College does not need to appoint a Data Protection Officer as it is not required to do so by law. Instead the College has a Data Protection Lead whose responsibilities include enabling the College to fulfil its mandatory data protection obligations. The Data Protection Lead role will be fulfilled by a member of College staff. The College will enable the effective performance of the DP Lead's tasks and ensure that they are given sufficient autonomy, time, resources and support to carry out their tasks effectively, including active support by senior management. The College will also ensure that the DP Lead is 'involved properly, and in a timely manner, in all issues which relate to the protection of personal data', that their opinion is given due weight and that they are consulted promptly once a data breach or another incident has occurred.

8. Responsibilities

8.1 The Senior Management Team will ensure that the purposes and means of processing personal data for which the College is data controller are determined in compliance with legislation. Responsibility for ensuring implementation of and compliance with this policy will be in accordance with the College's line management structure.

8.2 All individuals and organisations that process personal data on behalf of the College will comply with this policy and associated data protection, information security, information management and information technology regulations, policies, processes and procedures.

8.3 All employees / staff of the College are:

- responsible for their own compliance in processing personal data and other information. Non-compliance can result in disciplinary procedures.
- expected to be pro-active in seeking further information / knowledge to further their professional competence. Advice can be sought from the DP Lead.

8.4 Third parties processing personal data on behalf of the College will comply with this policy alongside any specific terms and conditions agreed contractually.

8.5 The Data Protection Lead is an advisory role working to ensure that Commonwealth Education Foundation complies with the requirements of current data protection legislation and regulatory requirements. The Data Protection Lead reports directly to the Rector. The DP Lead shall:

- inform and advise all members of staff on their obligation to adhere to data protection legislation and regulatory requirements when dealing with personal data
- monitor compliance with data protection legislation and regulatory requirements
- advise and inform on data protection impact assessments (DPIA), including monitoring performance of DPIAs against the requirements of data protection legislation and regulatory requirements.
- liaise and cooperate with the supervisory authority (the ICO). This requires an appropriate level of independence and must not be influenced by other roles at any level.
- be the point of contact for the supervisory authority on issues relating to processing of personal data, and to consult with the supervisory authority, where necessary, on any other personal data matters.
- contribute to the development and maintenance of all Commonwealth Education Foundation data

protection policies, procedures and processes in relation to the protection of personal data.

- advise the College's Senior Management on the allocation of responsibilities internally to support ongoing compliance with data protection legislation and regulatory requirements
- ensure training and awareness is available and delivered to all members of staff involved in processing operations relating to personal data
- regularly monitor compliance with data protection legislation and regulatory requirements by conducting audits of processes relating to personal data, and report to the Rector
- be the lead point of contact for data subjects with regard to the processing of their personal data including the facilitation of their rights
- monitor compliance with the Commonwealth Education Foundation Data Protection Policy and develop/advise on procedures for effective security
- advise senior management on the allocation of information security responsibilities
- develop/advise on formal procedures for personal data reporting incidents and investigations
- contribute to the business continuity and disaster recovery planning process
- advise on and monitor the safeguarding of organisational record management
- work with all business areas to ascertain the extent to which personal data is collected, held and/or used by the College, and that it is properly controlled and safeguarded from loss of confidentiality, integrity or availability from any cause
- advise the controller of its obligation to issue privacy notices to data subjects at the point of collection of their personal data under Articles 13 to 15
- plan and schedule data processing audits regularly, monitoring core activities to ensure they comply with the data protection legislation and regulatory requirements
- liaise with all members of staff on matters of data protection
- bring to the attention of the Rector any matters which are potential risk factors to the proper safeguarding of personal data within the College

8.6 The Data Protection Lead is authorised to have access to all of the College's systems relating to the collection, processing and storage of personal data for the purpose of assessing the use and security of personal data. The Data Protection Lead may expect the cooperation of all staff in carrying out these duties, including access to systems and records. In the event that cooperation is not forthcoming, the Data Protection Lead will report to the Rector or where necessary the Governing Board.

8.7 The Rector is an accountable role and is concerned with the management of all information assets held by the College. In relation to personal data, the Rector has overall responsibility for:

- the processing of personal data (of which the College is data controller) in compliance with data protection legislation, including the appropriate determination of the purposes of processing personal data, and the means by which any personal data processing activity is done
- ensuring that the DP Lead is involved properly, and in a timely manner, in all issues which relate to the protection of personal data, that the opinion of the DP Lead is given due weight and that the DP Lead is consulted promptly once a data breach or another incident has occurred
- the management of data protection risks

- planning, implementing and progressing the College's data protection initiatives
- managing the implementation of essential elements of data protection legislation, such as the principles of data processing, data subjects' rights, data protection by design and by default, records of processing activities, security of processing and notification and communication of data breaches
- managing the response to breaches of data protection legislation
- ensuring that an effective monitoring and reporting framework is established in relation to data protection compliance, and that information asset owners and super information asset owners are designated, perform their roles and report regularly on data protection compliance in relation to their respective information assets and business units
- ensuring that no individual is given access to personal data without having undertaken appropriate training and read relevant policy and guidance
- be pro-active in seeking further information / knowledge to further their professional development regarding data protection

8.8 The Rector shall also play a key role in fostering a data protection culture within the College.

9. Designated Data Protection lead

9.1 The College's designated Data Protection Lead is:

Shaiye Daniel
Email: dataprotection@christredeemer.ac.uk

10. Training

10.1 The College is committed to providing adequate data protection training to its employees in order to help protect the rights and freedoms of individuals in accordance with the provisions of the GDPR and DPA 2018.

10.2 All employees of the College whose work involves accessing personal data shall:
- be informed of the expectation that they will follow the Data Protection Policy and its associated policies and procedures. This expectation will also form part of the contract of employment.
- be required to undertake the College's data protection training. If an employee declines to undertake the training, the College will investigate and where the reason for this is deemed unacceptable this may result in disciplinary proceedings.
- Be provided with appropriate training and / or clear procedures for compliant processing of personal data according to their role.

10.3 For casual staff such as agency temps, whose role may involve accessing personal data, the onus is on managers to ensure that such staff are aware of their responsibilities.

10.4 It is the responsibility of a line manager to ensure their staff undertake the relevant training.

10.5 All employees whose work does not ordinarily involve accessing personal data will be given bespoke training and / or required to follow data protection procedures relevant to their role. This includes employees and casual workers such cleaners, maintenance, security staff and student volunteers.

11. Data Breaches

11.1 Any data breaches or suspected data breaches should be immediately managed and reporting in accordance with the Data Breach Incident Response and Reporting Procedure (for staff and students) available on the VLE. Data breaches or suspected data breaches should be reported to the College by emailing dataprotection@christredeemer.ac.uk. Breaches will be managed in accordance with the Data Breach Incident Response and Reporting Procedure (for DP Lead), which includes, where necessary, notifying the ICO within 72 hours of a breach being known.

12. Breaches of Policy

12.1 Failure to follow any of the applicable College policies by staff / employees may result in disciplinary action. A data breach by a third party may result in a termination of contract and/or compensation claim.

13. Approval and Review

Title: Data Protection Policy
Approved with reference to: QAA Quality Code.
Version: 2020.1. **Approved:** August 2020. **Implementation from:** August 2020. **Next review:** August 2021.
Approving body: Audit Committee. **Member of staff responsible:** Compliance and HR Manager