TRINITY COLLEGE BRISTOL

DATA PROTECTION POLICY

1.0 Policy statement

1.1 Trinity College Bristol is committed to protecting the rights, freedoms and privacy of individuals for whom we hold and process personal data by adhering to the provisions of the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) and promoting best practice.

1.2 The College processes information about individuals with whom we have dealings, for our administrative purposes and to comply with our legal and contractual obligations. Such information includes personal data held by the College on staff and students (or prospective staff and students) and others relating to the College, including members of Council and committees, friends and members of the Association, occasional lecturers, suppliers and contractors, day nursery parents and children, and others, in order to enable us to carry out our function as a theological college.

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

i. employees, consultants, contractors and temporary workers;
ii. students undertaking a programme of study and also students performing paid or voluntary work for the college;
iii. arms' length organisations associated with, and officially recognised by, the college; and
iv. third parties associated with the college.

1.4 The College, as a data controller, acknowledges its responsibility and need to demonstrate compliance with the principles of data protection legislation. We affirm our commitment to adopt and to develop good practice in relation to the principles governing the processing and storing of personal data contained in the provisions of the Act and the GDPR. All personal data held by the College shall be:

i. processed lawfully, fairly and in a transparent manner in relation to individuals;
ii. 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, historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
iii. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
iv. accurate and, where necessary, kept up to date; every reasonable step shall 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;
v. 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 shall be stored for longer periods insofar as the personal data shall be processed solely for archiving purposes in the public interest, historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
vi. 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.

1.5 We uphold the right of individuals granted under data protection legislation to:

i. be made aware at the point of data collection of how their personal data is to be used
ii. access their personal data so that they are aware of and can verify the lawfulness of the data processing, as well as have any inaccuracies in the data corrected
iii. have personal data rectified where there is inaccurate or incomplete data
iv. request in certain circumstances the deletion or removal of personal data where there is no compelling reason for continued processing of the data
v. ask that the processing of their personal data be temporarily halted in certain circumstances whilst a review is undertaken of such processing

2.0 Practice

2.1 In practice, the College will:

i. undertake a data protection impact assessment screening for any new initiatives that involve the sharing of personal data;
ii. identify a clear objective, or set of objectives, for the sharing of personal data;
iii. identify a lawful basis in data protection legislation for the sharing of personal data;
iv. ensure that the sharing of personal data is necessary to achieve the identified objective(s); anonymised or pseudonymised data shall be shared where the identification of data subjects is not required;
v. share the minimum amount of personal data required to achieve the objective(s);
vi. provide data subjects with privacy notices and, where data subjects have a choice, seek consent for the sharing of their personal data;
vii. clearly distinguish factual information from opinions;
viii. record all decisions to share personal data;
ix. ensure that a written agreement between the parties to a data sharing arrangement is in place where personal data is shared on a systematic basis;
x. processes and procedures are in place for handling information security incidents;
xi. promote good practice by drawing on the experience of other organisations, reflecting on current practice, and fostering a positive attitude towards the careful handling of personal data.

3.0 Responsibility

3.1 The Data Controller is Trinity College Bristol.

3.2 The College Council delegates to the Senior Management Team responsibility for monitoring and ensuring implementation of the Data Protection Policy and for ensuring that a data protection culture is fostered in the College.

3.3 The Executive Director acts on behalf of the SMT as the lead person with responsibility for developing policy and ensuring implementation.

4.0 Data Breach

4.1 Any breach of this policy should be reported as soon as possible to the Executive Director's office. This includes any information security incident that has affected the confidentiality, integrity or availability of data.

4.2 A data breach is a breach of security leading to the unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, data. It may be accidental or deliberate.

4.3 A breach of this policy by an employee or student may result in disciplinary action. A breach by a third party may result in a termination of contract and/or a compensation claim.

5.0 Complaints

5.1 Where there is dissatisfaction with the way in which the College processes an individual's personal data, the individual is invited to contact the Executive Director's office in the first instance in order that the matter can, if possible, be addressed and rectified. In the event that the matter cannot be satisfactorily resolved, the matter can be referred to the Information Commissioner's Office (ICO) at Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF; tel 0303 123 1113; web: ico.org.uk.

6.0 Review

6.1 This policy shall be reviewed by the college's Senior Management Team annually or whenever there is a significant change in legislation, strategy or organisation. Major changes shall be approved by the College Council.