TRINITY COLLEGE BRISTOL

DATA PROTECTION POLICY

The Council of Trinity College Bristol affirms its commitment to adopt and to develop good practice in relation to the eight principles governing the processing and storing of personal data contained in the Data Protection Act 1998. All 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 and contractors, day nursery parents and children, shall be:

1. processed fairly and lawfully and in accordance with the conditions of the Act;

2. obtained only for specified purposes and shall not be further processed in any manner incompatible with those purposes;

3. adequate, relevant and not excessive in relation to the purpose for which they are held;

4. accurate and, where necessary, kept up to date;

5. kept for no longer than is necessary for the purposes of their being processed;

6. processed in accordance with the subject access rights laid down by the Act;

7. held securely to prevent unauthorised or unlawful processing or accidental loss, destruction or damage;

8. transferred outside the European Economic Area only where an adequate level of protection is ensured in relation to the processing of personal data (or in such circumstances where the College is entitled under contract or by law to transmit such data or has received the explicit consent of the data subject).

Recognising that the College, in view of the nature of its charitable objects, is bound to hold sensitive personal data, in particular in relation to religious affiliation, the College further affirms its commitment to:

1. process such data only in the course of its legitimate activities;

2. ensure appropriate safeguards are in place for the rights and freedoms of data subjects; and

3. disclose such data to third parties only where consent has been obtained, except in so far as the Act confers an obligation or right on the College to do otherwise. In particular, the College will not seek explicit consent for the processing of data needed to perform its contract with the data subject.

/continued ….

In practice, the College will:

1. seek to ensure that no personal data are given to people outside the College without the consent of the person concerned;

2. obtain written consent from the person concerned before sensitive personal information is released to those who are not a party to the contractual arrangement between the College and the data subject;

3. withdraw and securely dispose of information held on personal files by the end of a five year period following the departure of the person concerned from the College and to keep beyond this period only such information that is deemed by the College to have continuing relevance, including that of archival value.

4. restrict use of personal data within the College to staff who in the course of their legitimate duties require access to the information or to others in the College who receive specific and appropriate authorisation.

5. notify College staff and students in general terms of the kind of personal data held on them and the purposes for which they are held and processed.

6. inform College staff and students of the right of access given to them under the Act to information held on them by the College.

7. comply with requests for data subject access within a period of 40 days subject to a fee of £10.

8. take all reasonable steps to ensure that all those who supply the College with reports, references or other personal information or opinion are aware of their duty of care to the College and the data subject and of the data subject's access rights.

9. take care to secure the privacy of all individuals associated with the College.

10. protect the rights of third parties to privacy, withholding where necessary personal data relating to third parties from data subject access requests.

11. ensure that all applicants to the College are aware of the College's data protection policy and that agreement to operate within the terms of the policy is a condition of engagement.

12. delegate to the Senior Management Team responsibility for monitoring and ensuring implementation of the Data Protection Policy.

13. 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.

Adopted 19.11.2001
Approved by Council December 2015