ST AUGUSTINE'S
COLLEGE OF THEOLOGY

St Augustine's Data Protection Policy

The 1998 Data Protection Act is designed to protect the rights of individuals concerning information or personal data held about them. From May 2018 this has been enhanced with GDPR (General Data Protection Regulation). As a registered student of St Augustine's, and in order to meet the requirements of sponsoring and funding bodies, and our partner university (Durham) it is necessary for the College to hold data in both written and electronic form on you – and the lawful basis in which we collect this information.

1 Introduction – Data Protection Principles

1.1 When handling such information, the College, and all staff or others who process or use any personal information, must comply with the Data Protection Principles set out in the Act. In summary, these state that personal data shall be

1.2.1 processed fairly and lawfully

1.2.2 obtained for specified and lawful purposes and not further processed in a manner incompatible with those purposes

1.2.3 adequate, relevant and not excessive

1.2.4 accurate and, where necessary, up to date

1.2.5 kept for no longer than necessary

1.2.6 processed in accordance with data subjects' rights

1.2.7 protected by appropriate security

1.2.8 not transferred to a country outside the European Economic Area without adequate protection

2 Registration

2.1 To comply with the Act, the College makes an entry in the Data Protection Register maintained by the Information Commissioner. Details of the College's current entry

in the Data Protection Register are available on the Information Commissioner's web site (https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/). The Registration Number is ZA243971.

2.3 The College notified the Information Commissioner that we process personal information to enable us to provide education and support services to our students and staff; advertising and promoting and alumni relations.

4 Responsibility for Data Protection

4.1 The College is the Data Controller under the Act. The Governing Body is ultimately responsible for ensuring compliance.

5 Notification of Data Held and Processed

5.1 All staff, students, and other users are entitled to:

5.1.1 know what personal information the College holds and processes about them and why

5.1.2 know how to gain access to it

5.1.3 know how to keep it up to date

5.1.4 know what the College is doing to comply with its obligations under the Act

6 Staff Guidelines for Data Protection

6.1 All members of staff are responsible for:

6.1.2 informing the College of any changes to information they provided, for instance changes of address and qualifications

6.1.4 informing the College of any errors or, where appropriate, follow procedures for up-dating entries

7 Data Security

7.1 All members of staff are responsible for ensuring that:

7.1.1 any personal data that they hold, whether in Electronic or Paper format, is kept securely

7.1.2 personal information is not disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party

7.3 Unauthorised disclosure may be a disciplinary matter.

7.4 All members of staff and students dealing with data should ensure that casual access to data is not possible, for example by members of the public seeing VDU screens or printouts. VDU screens should be cleared after use, and terminals should not be left unattended without being logged off. Printouts should be kept securely, and shredded when no longer required. Particular care must be taken when laptop computers are used in public places or on public transport, and when working at home.

7.5 All members of staff and students dealing with data should hold appropriate back up or duplicate copies of data, in case of unauthorised destruction or loss of data.

7.6 All data breaches need reporting immediately to the Data Protection Officer.

10 Subject Consent to Processing Sensitive Information

10.1 The College may ask for information about a person's particular health needs and disabilities for use in providing appropriate support for the individual especially with regard to planning residential events.

12 Rights to access information

12.1 Staff, students, and other users of the College facilities have the right to access any personal data that is being kept about them in a relevant filing system. Any person who wishes to exercise this right should make their request in writing to the Data

Protection Officer. The fee of £10, which is the statutory charge, must accompany the application.

12.2 The College aims to comply with requests for access to personal information as quickly as possible. It will ensure its provision within 40 days from the receipt of the fee and proving evidence of identity.

13 Retention of Data

13.1 The College retains information in line with financial, legal, or archival requirements.

14 Data Protection Officer

14.1 St Augustine's Data Protection Officer is Rebecca Young