## Introduction

The College is registered with the Information Commissioner's Office (ICO) as Assemblies of God Bible College. The College is part of Assemblies of God Incorporated which is the data controller for all personal data that it holds and processes. However, because of its role as a Higher Education Provider (HEP), the College may collect, hold and process data on different legal bases, and issues relating to the control of data should, in the first instance, be directed to the College.

## Data Protection Lead

AoG Inc and the College each have a Data Protection Lead. The College's Lead is:

Mark Button
Vice Principal (Academic)
Missio Dei College
Ground Floor 1-2 The Cottages
Deva Centre
Trinity Way
Manchester
M3 7BE
email: mbutton@missiodei.ac.uk
Tel: 01777 817663

The College Data Lead should be the first point of contact for issues relating to College control of data, and data protection issues.

## Legal Basis

In general, the College holds and processes personal and some special category data primarily in order to enter into or to fulfil its contract with (potential) students as a HEP. In some situations data may also be held and processed as part of the College's legal obligation as a HEP and in order to protect the vital interests of data subjects. Use of data for any other purpose will be with the express consent of the subject(s) of the data for the data to be used for that purpose.

In order to fulfil its contract with students, the College may collect, hold and process personal data – including personal details, family and social circumstances, education and training records, employment information, financial details – and some special category data including racial or ethnic origin, religious or philosophical beliefs and data relating to physical or mental health. The College will also keep data relating to academic performance and potential future employment. All data will be processed only in order for the College to implement and manage services and support in relation to students, including recruitment, admission, registration, teaching and learning, examination,

graduation, accommodation, student support, including support for those with learning, mental health, and other disabilities, and careers guidance. The College also has an obligation, as a HEP, to share data with external agencies (see Availability of data to third parties, below).

All collecting and processing of data will be lawful, proportionate, fair and transparent, and will be necessary for the College to fulfil its contractual obligations. Where data is used for reporting and monitoring purposes, it will be anonymised wherever possible.

The College will collect the least amount of personal data necessary to provide its services, effectively. Data collected under one legal basis will not be used for another purpose, without identifying another legal basis for doing so. And, where necessary, further consent will be obtained. The College will check, and, where necessary, update data regularly to ensure its accuracy.

**Collection and storage of data**

Personal data and sensitive personal data/special category data held by the College relating to students will generally be obtained directly from the student or applicant, or in some cases from third parties, as authorised by (potential) students, for example data relating to AP(E)L or references required prior to admission.

Student data will generally be held in a form that identifies the subjects of the data for no longer than is necessary. Because information will be required beyond the period of study (e.g. for transcripts, references, etc.) this will normally be for a period of six years after the end of the period of study, unless there is a legal requirement for it to be held for longer, in which case it will be held for that longer period.

Student data in all formats will be stored securely, in such a way as to protect it from accidental loss, damage or destruction and unauthorised or unlawful access and use.

**Availability of data within AoG and to third parties**

Some data, including but not restricted to Finance, Health and Safety, access, dietary issues, complaints, disciplinary and safeguarding issues may be made available from time to time to appropriate AoG Inc staff, who share responsibility for student well-being.

The College will ensure that personal data is accessible only to those with a legitimate reason for using it, and that those with such legitimate access to personal data do not disclose to any unauthorised third parties.

The College may disclose student's personal and special category data to external agencies to which it has obligations, including local and central government, immigration authorities, the Police and security agencies, Office for Students (OfS), the Higher Education Statistics Agency (HESA), the Student Loans Company (SLC), and the Office of the Independent Adjudicator for Higher Education (OIA). It may also disclose relevant information to its validating University (currently the University of Chester), examining bodies and other regulatory authorities. These bodies have their own Data Protection policies, which ensure a legal basis for their processing of information. These policies are available on request.

If students have unpaid debts at the end of their course AoG Inc may, at its discretion, pass this information to debt collecting agencies in order to pursue the debt.

Contact details may be passed on to bodies conducting legitimate surveys, including the National Student Survey (NSS).

In other cases, personal and special category data will not be made available to third parties except with the explicit, demonstrable consent of the subject(s) of the data.

As an employer, AoG Inc., has the right to access e-mails from or to employees, for the purposes of system management and security. This is carried out on the legal basis of 'legitimate interest'. However, because some e-mails may contain personal and sensitive student information, which needs to be protected, the following safeguards are in place.

- There is no routine monitoring of e-mails. Monitoring may only be carried out where there is a demonstrable legitimate interest.
- Before any monitoring takes place, an assessment will be conducted into the scope of the monitoring, why it is necessary, and the risks associated with it.
- Board of Director level authorisation will be required to conduct such monitoring.
- The Data Protection Lead for the College will be notified both of the intention to monitor and of the identity of those who will be carrying out the monitoring, in order to ensure that personal student data is not accessed by unauthorised third parties.
- Any personal data relating to students accessed while monitoring staff e-mails is not processed, not disclosed to any third party, and held only as long as necessary.
- Students including sensitive personal data in e-mails to the College are encouraged to do the following:
    - Include data in an attachment to the e-mail, rather than in the body of the e-mail text.
    - Include the word CONFIDENTIAL in the e-mail subject line.

**Student rights relating to personal and special category data**

Under the GDPR, individuals whose data is held by the College have the right:

- To request access to their personal data held by the College.
- To have inaccurate or incomplete personal data rectified.
- To have data erased where the College has no legitimate reason to keep it.
- To object to or restrict the processing of personal data in particular situations.
- To data portability, i.e. to have some elements of their information (e.g. academic performance details) sent digitally to other organisations.
- Not to be subject to a decision based solely on automated processing.
- Where the processing of personal or special category data is based on the consent of the student, to withdraw that consent at any time.

All requests to exercise any of these rights should be made to the College Data Protection Lead. In some cases, templates are available on request.

Information about action taken in response to students exercising rights under the GDPR will be given 'without due delay and in any event within one month of receipt of the request'.

Further, if a student believes that the College's processing of personal and special category data is not lawful, proportionate, fair and transparent, is not being used in accordance with this policy, or that the requirements of the GDPR may not be fully complied with, he or she should contact the College's Data Protection Lead in the first instance. If that does not lead to a satisfactory resolution, the College's formal complaints procedure could be invoked.

**Information relating to data processing**

The College will provide information about the purpose for which data is collected and the period for which the data will be stored to the subject(s) of the data, at or before the time of collection, 'in a concise, transparent, intelligible and easily accessible form, using clear and plain language'.

The College recognises that sensitive, personal data may be made available to staff in a particular context. Examples may include information given to academic staff in relation to extensions or mitigating circumstances, or to the College pastoral team – which includes the Disability Officer. Any such data will, generally, be kept within that department, unless sharing between departments is necessary for us to fulfil our contractual responsibilities, or consent may be assumed to have been given. For example the Disability Officer will need to disclose information about Needs Assessments to the academic department and to lecturers in order to ensure that students receive appropriate support. Such disclosure will, though, be proportionate, and in order to meet the needs of students.

For any questions or clarifications please contact the College Data Protection Lead.