



Missio Dei
Leadership & Theological College

ASSEMBLIES OF GOD BIBLE COLLEGE (MISSIO DEI COLLEGE) – DATA PROTECTION POLICY

Introduction

On 25 May 2015, the Data Protection Act 1998 (DPA), which up until then regulated the processing of personal and sensitive personal data,¹ was superseded by the General Data Protection Regulation (GDPR).² This provides individuals with enhanced rights, and imposes increased responsibilities on organisations processing personal and special category data.³ This policy statement sets out the procedures that govern the collection, storage, availability and erasure of student data under GDPR. This policy complements the more general data protection policy of AoG Inc. and should be read in conjunction with it.

Missio Dei (MD) is registered with the Information Commissioner's Office (ICO) as Assemblies of God Bible College, though, since MD is the more common title, that is how it will be referred to in this document. MD is part of Assemblies of God Inc., which is the Data Controller for all personal data that it holds and processes. However, because of its role as a HE provider MD 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 MD. AoG Inc. and MD each have a Data Protection Lead. MD's Data Protection Lead is, currently:

Mark Button,
Assemblies of God College,
Ground Floor & Floor 2,
No. 1-2 The Cottages, Deva Centre,
Trinity Way,
Manchester,
M3 7BE

Email: mbutton@matterseyhall.com
Tel. 01777 817663 ext. 22

¹ 'Personal data' refers to any information relating to a living individual; 'processing' is any activity carried out involving personal data, including holding and storing.

² For a guide to GDPR, see <https://ico.org.uk/for-organisations/guide-to-the-general-dataprotection-regulation-gdpr/>; <https://www.eugdpr.org/the-regulation.html>.

³ 'Special category data' replaces 'sensitive personal data' (which was the term under DPA).



Missio Dei

Leadership & Theological College

Legal Basis

The GDPR gives six possible legal bases for collecting, holding and processing data.⁴ In general, MD 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 Higher Education Provider (HEP). In some situations data may also be held and processed as part of MD's legal obligation as an 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.⁵

In order to fulfil its contract with students, MD 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. MD will also keep data relating to academic performance and potential future employment. All data will be processed only in order for MD 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. MD also has an obligation, as an 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 MD to fulfil its contractual obligations. Where data is used for reporting and monitoring purposes, it will be anonymised wherever possible.

⁴ GDPR, Article 6, 'Lawfulness of Processing'. These are: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. (GDPR, Article 6(1)).

⁵ Consent is defined as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her' [Articles 4(11); 7(2-3)]. In this regard, the request for consent must be 'in an intelligible and easily accessible form, using clear and plain language' [GDPR, Article 7(2)]. The GDPR also expressly requires that 'the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data' [GDPR, Article 7(1)].



Missio Dei

Leadership & Theological College

MD will collect the least amount of personal data necessary to provide its services, effectively.⁶ Data collected under one legal basis will not be used for another purpose, without identifying another legal basis for doing so.⁷ And, where necessary, further consent will be obtained. MD 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 MD 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 may be required beyond the period of study (e.g. for transcripts, references, etc.) this will normally be for a period of six years, 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.⁸

Availability of data to third parties

MD 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, the Higher Education Statistics Agency (HESA),⁹ 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.

⁶ GDPR, Articles 5(1)(c), 25(2).

⁷ GDPR, Article 5(1)(b).

⁸ Provision for the security of data, data breaches, etc. is included in the Data Protection provision of Assemblies of God Inc. and is available via their website.

⁹ For details of HESA data collection, including the categories of data, its use and protection issues, see <https://www.hesa.ac.uk/about/regulation/data-protection/notices>.



Missio Dei

Leadership & Theological College

If students have unpaid debts at the end their course MD 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).

Some data, primarily relating to dietary issues, accommodation, access, Finance, Health and Safety, Campus Management, complaints and disciplinary issues may be made available to appropriate National Ministry Centre staff, who share responsibility for student well-being.

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.

MD 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 disclosed to any unauthorised third parties.

As employer of Missio Dei staff, AoG Inc., has the right to access e-mails from or to employees,¹⁰ for the purposes of system management and security. This is carried out on the legal basis of 'legitimate interest'.¹¹ However, because some e-mails may contain personal and sensitive student information, which needs to be protected,¹² 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 into the scope of the monitoring, why it is necessary, and the risks associated with it will be conducted.
- The authorisation of the Directors of AoG Inc. to conduct such monitoring is also required.
- The Data Protection Lead for MD 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.

¹⁰ This applies only to AoG Inc. and MD e-mail addresses. There is no right to access communication to or from other personal e-mail addresses.

¹¹ GDPR,

¹² In such cases, students whose personal information may be accessed along with employee e-mails, become, inadvertently, the data subject, whose 'fundamental rights and freedoms' ... 'which require protection of personal data' override the legal basis of 'legitimate interest'.(GDPR, Article 6(1)(f)).



Missio Dei

Leadership & Theological College

- 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 MD staff 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 MD have the right:

- To request access to their personal data held by MD.¹³
- To have inaccurate or incomplete personal data rectified.¹⁴
- To have data erased where MD has no legitimate reason to keep it.¹⁵
- To object to or restrict the processing of personal data in particular situations.¹⁶
- To data portability, i.e. to have some elements of their information (e.g. academic performance details) sent digitally to other organisations.¹⁷
- Not to be subject to a decision based solely on automated processing.¹⁸
- Where the processing of personal or special category data is based on the consent of the student, to withdraw that consent at any time.¹⁹

All requests to exercise any of these rights should be made to the 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'.²⁰

Further, if a student believes that MD'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 MD's Data Protection Lead in the first instance. If that does not lead to a satisfactory resolution, MD's formal complaints procedure could be invoked.

¹³ GDPR, Article 15

¹⁴ GDPR, Article 16

¹⁵ GDPR, Article 17

¹⁶ GDPR, Articles 21, 18

¹⁷ GDPR, Article 20

¹⁸ GDPR, Article 22

¹⁹ Where consent is withdrawn, that withdrawal must be implemented across all data processing systems [GDPR, Article 7(3)].

²⁰ GDPR, Article 12(3)



Missio Dei
Leadership & Theological College

Information relating to data processing

MD 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'.²¹

MD 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 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 MD Data Lead.

MB – revised, July 2020

²¹ *GDPR, Article 12(1)*