Data Protection		
	Policy Name:	Data Protection
	Policy Reference	Gov02
	Applies To:	AoG Inc.
	Approved By:	Board of Governors
	Approval Date:	18/09/20
	Next review Date:	September 2020
	Policy Lead:	Operations Manager
	Policy Contact:	policy@aog.org.uk

PART 1 – Policy Statement:

AoG Inc. is committed to the highest standards of data management through policy and procedural management to meet the needs of the organisation and support the outworking of the National Leadership Team's Vision.

Background/Introduction/Statement/Preamble

General Data Protection Regulation 2018

This legislation came into force on the 25th May 2018 and replaced The Data Protection Act 1998. The GDPR regulates the processing of personal data, and protects the rights and privacy of all living individuals (including children), for example by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request'.

The College data protection procedures are included within this company policy. Their policy statement sets out the procedures that govern the collection, storage, availability and erasure of student data under GDPR. It is appended to this policy.

Security Statement

AoG Inc has taken measures to guard against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage. This includes:

- Adopting an information security policy (this document is the AoG Inc and Bible College policy, and the College have a college-specific policy that sits alongside this one)
- Taking steps to control physical security (projects and staff records are all kept in locked cabinets);
- Recommending procedures that reduce the requirement to send sensitive documentation via email (eg using the "Shared Drive" to access a single version, use of secure cloud storage etc);
- Putting in place controls on access to electronic information (password protection on files (where appropriate) and limited server access);
- Recommending mobile equipment is password protected, and personal and work data is kept separate where possible;
- Ensuring any personally-identifiable data is kept completely confidential and must not be made available to any agency or individual without the formal and prior approval of the data controller's designated lead;
- Establishing a business continuity/disaster recovery plan (AoG Inc & Bible College take regular back-ups of its computer data files and this is stored away from the office at a safe location);

- Training all staff on security systems and procedures as appropriate;
- Detecting, investigating and reporting breaches of security should they occur.

Definitions

Legal bases for processing: The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever AoG Inc process personal data:

(a) Consent: the individual has given clear consent to process their personal data for a specific purpose.
(b) Contract: the processing is necessary because of a contract with the individual, or because they have asked you to take specific steps before entering into a contract.
(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
(d) Vital interests: the processing is necessary to protect someone's life.
(e) Public task: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.
(f) Legitimate interests: the processing is necessary for legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if it is a public authority processing data to perform the organisation's official tasks.)

Personal data: information relating to an individual and may be in hard or soft copy (paper/manual files; electronic records; photographs; CCTV images), and may include facts or opinions about a person.

Functionary: any person carrying out a function for or on behalf of AOG Inc or whose actions will reflect on AOG Inc including without limitation all employees of AOG Inc, any self-employed person or person supplying services to AOG Inc under a contract for services, any other person engaged for any purpose connected with AOG Inc whether on a paid or voluntary basis

Scope (if relevant)

<u>Contract as a basis for processing</u>

AoG Inc understands contract to include contracts with students who apply to and are accepted onto any educational course; contracts with individuals and churches who apply for and are commissioned with AoG status; contracts with AoG Churches that utilise the AoG Gift Aid service; contracts with third parties for services.

<u>Legitimate Interest as a basis for processing</u>

AoG Inc understands legitimate interest to include work undertaken by functionaries on behalf of a specific team or department, for example voluntary roles, where AoG's legitimate interest in processing is balanced against the rights of the data subject, and the individual has freely and expressly signified their agreement.

<u>Consent as a basis for processing</u>

Although it is not always necessary to gain consent from individuals before processing their data, it is often the best way to ensure that data is collected and processed in an open and transparent manner. Consent is especially important when AoG Inc is processing any sensitive data, as defined by the legislation. (See Appendix 1)

AoG Inc understands consent to mean that the individual has been fully informed of the particular purpose for requesting consent, the intended processing and has signified their agreement (e.g. via an application or enrolment form) whilst being of a sound mind and without having any undue

influence exerted upon them. Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.

AoG Inc will ensure that any forms used to gather data on an individual will contain a statement (fair collection statement) explaining the use of that data, how the data may be disclosed and also indicate whether or not the individual needs to consent to the processing.

AoG Inc will ensure that if the individual does not give his/her consent for the processing, and there is no other lawful basis on which to process the data, then steps will be taken to ensure that processing of that data does not take place.

Objectives/Purpose

AoG Inc. (including the College) undertakes to adhere to the eight principles:

1) Process personal data fairly and lawfully.
2) Process the data for the specific and lawful purpose for which it collected that data and not further process the data in a manner incompatible with this purpose.
3) Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed.
4) Keep personal data accurate and, where necessary, up to date.
5) Only keep personal data for as long as is necessary.
6) Process personal data in accordance with the rights of the data subject under the legislation.
7) Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data.
8) Ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Roles & Responsibilities

Data Control Responsibility

Assemblies of God Incorporated is the data controller under the terms of the legislation, which means it is ultimately responsible for controlling the use and processing of the personal data. There are Data Protection Leads appointed in two operational areas: Assemblies of God GB Inc. and the College (currently trading as Mattersey Hall Bible College) with data protection leads that operate independently. There is a nominated Director who oversees the policy.

All "functionaries" (staff, volunteers and third parties) of AoG Inc. who process personal information have personal responsibility to comply with the legislation.

Individuals who provide personal data to AoG Inc. are responsible for ensuring that the information they provide is accurate and up-to-date.

All management, staff and volunteers - cooperation is needed and expected from everyone, working as a team with common goals and objectives to ensure the success of this data protection policy.

PART 2 – Version History of the Policy:

Policy Author	Version #	Summary of Changes
Operations Mngr	1.0	New Document

PART 3 – Procedures & Areas of Work

3.1 Data Control

Both AoG Inc and College use the identical process for paying the Information Commissioner's Office each year. Whilst the registration does not require specific data 'purposes', the areas of work are currently listed as follows:

Assemblies of God GB Inc.

- Accounts and records
- Advertising, marketing and public relations
- Staff administration
- Administration of membership records
- Trading/sharing in personal information
- Fundraising
- Realising the objectives of a charitable organisation or voluntary body
- Accounting & Auditing
- Pastoral Care
- Other Commercial Services
- Crime Prevention and Prosecution of Offenders

See Appendix 1 for full details of all purposes

Assemblies of God Bible College

- Staff, Agent and Contractor Administration
- Advertising, Marketing, Public Relations, General Advice Services
- Accounts & Records
- Education
- Student and Staff Support Services
- Research
- Other Commercial Services
- Crime Prevention and Prosecution of Offenders

3.2 Hard Copy Personal Data:

AoG Inc will have in place appropriate security measures e.g. ensuring that hard copy personal data is kept in lockable filing cabinets/cupboards with controlled access (with the keys then held securely in a key cabinet with controlled access):

- keeping all personal data in a lockable cabinet with key-controlled access.
- password protecting personal data held electronically.
- archiving personal data which are then kept securely (lockable cabinet).
- placing any PCs or terminals, CCTV camera screens etc. that show personal data so that they are not visible except to authorised staff.
- ensuring that PC screens are not left unattended without a password protected screen-saver being used.

In addition, AoG Inc will put in place appropriate measures for the deletion of personal data - manual records will be shredded or disposed of as 'confidential waste' and appropriate contract terms will be put in place with any third parties undertaking this work. Hard drives of redundant PCs will be wiped clean before disposal or if that is not possible, destroyed physically. A log will be kept of the records destroyed.

3.2 Working from Home:

This policy also applies to functionaries who process personal data 'off-site', e.g. when working at home, and in circumstances additional care must be taken regarding the security of the data.

- Functionaries are expected to make every effort to use secure methods of work that eliminate or minimise local processing and storing (for example use of the AoG "Shared Drives");
- The Data Controller (AoG Inc or Bible College Lead) will keep record of which functionary regularly takes work home with them;
- If working on something at home and at work, both sets of information should be kept up to date (applies to AoG Inc and Bible College);
- Home computers should have records removed once project/work records are no longer needed at home, links to cloud or remote working software, and passwords must be changed and accounts blocked (applies to AoG Inc and Bible College).
- Functionaries must agree to try to keep work taken home secure, to return all work related material upon the completion /termination of their contract; and the organisation should be informed immediately if information has got into wrong hands.

3.3 Subject Access Rights:

Individuals have a right to access any personal data relating to them which are held by AoG Inc. Any individual wishing to exercise this right should apply in writing to the appropriate Data Protection Lead. Any member of staff receiving a SAR should forward this to the appropriate Data Protection Lead.

Under the terms of the legislation, any such requests must be complied with within 40 days.

3.4 Disclosure of Data:

- Only disclosures which have been notified either under specific Privacy Notices or within the Privacy Policy must be made and therefore functionaries should exercise caution when asked to disclose personal data held on another individual or third party.
- AoG Inc undertakes not to disclose personal data to unauthorised third parties, including family members, friends, government bodies and in some circumstances, the police.
- Legitimate disclosures may occur in the following instances:
    - the individual has given their consent to the disclosure;
    - the disclosure is reasonably expected and in the legitimate interests of all parties;
    - the disclosure has been notified to the Information Commissioner's Office and is in the legitimate interests of AoG Inc;
    - the disclosure is required for the performance of a contract.
- There are other instances when the legislation permits disclosure without the consent of the individual.
- In no circumstances will AoG Inc. sell or give any of its databases to a third party.

3.5 Publication of Information:

AoG Inc may from time to time publish various items which may include some personal data, e.g.

- internal telephone directory.
- event or marketing information.
- photos and information in marketing materials.
- AoG Status Church & Minister "Yearbook"

It may be that in some circumstances an individual wishes their data processed for such reasons to be kept confidential, or restricted access only. Therefore it is AoG Inc policy to consider offering an opportunity to opt-out of the publication of such when collecting the information, unless it would

undermine the essential terms of the contract between AoG Inc as accrediting body and the person receiving accreditation, as summarised in the Articles and other constitutional documents.

3.6 Email:

It is the policy of AoG Inc to ensure that senders and recipients of email are made aware that under GDPR regulation, the contents of email may have to be disclosed in response to a request for information. One means by which this will be communicated will be by a disclaimer on the organisation's email. Under the Regulation of Investigatory Powers Act 2000, Lawful Business Practice Regulations, any email sent to or from a functionary may be accessed by someone other than the recipient for system management and security purposes.

3.7 CCTV:

There are some CCTV systems operating within AoG Inc (at Mattersey) for the purpose of protecting residents, visitors, staff and property. AoG Inc will only process personal data obtained by the CCTV system in a manner which ensures compliance with the legislation.

3.7 Special funding tracking requirements and data protection:

Where grant or other funding has specific requirements, the following principles apply:

- Try not to keep more than project/tracking requires;
- The more information kept, the more secure it should be kept;
- If publishing volunteers' details, tell them;
- Take extra care if records include sensitive data;
- Just keep personal data as long as necessary under funding rules;
- Don't keep surplus information.

3.8 Procedure for Review

This policy will be updated as necessary to reflect best practice or future amendments made to the General Data Protection Regulation (GDPR) May 2018. Please follow this link to the ICO's website (www.ico.gov.uk) which provides further detailed guidance on a range of topics including individuals' rights, exemptions from the Act, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc. In particular, you may find it helpful to read the Guide to Data Protection which is available from the website.

PART 4 – Linked Policies:

Policy	Number #	Summary
Subject Access Request	Gov04	Subject access request & form

PART 5 – Appendices:

Number #	Appendix Name
1	Data Protection Principles
2	Special Category Data
3	College
4	Purposes

APPENDIX 1 - DATA PROTECTION PRINCIPLES

The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles. Please follow this link to the ICO's website (www.ico.gov.uk). In order to comply with its obligations, AoG Inc. (including the College) undertakes to adhere to the eight principles:

1) Process personal data fairly and lawfully.

- AoG Inc will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

2) Process the data for the specific and lawful purpose for which it collected that data and not further process the data in a manner incompatible with this purpose.

- AoG Inc will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.

3) Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed.

- AoG Inc will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind. If any irrelevant data is given by individuals, it will be destroyed immediately.

4) Keep personal data accurate and, where necessary, up to date.

- AoG Inc will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify the relevant part of AoG if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of AoG Inc to ensure that any notification regarding the change is noted and acted on.

5) Only keep personal data for as long as is necessary.

- AoG Inc undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means the relevant part of AoG will undertake a regular review of the information held and implement a review, retention and disposal process.
- AoG Inc will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste). A log should be kept of the records destroyed.

6) Process personal data in accordance with the rights of the data subject under the legislation.

- Individuals have various rights under the legislation including a right to:
  - be told the nature of the information AoG Inc holds and any parties to whom this may be disclosed.
  - prevent processing likely to cause damage or distress.
  - prevent processing for purposes of direct marketing.
  - be informed about the mechanics of any automated decision-taking process that will significantly affect them.
  - not have significant decisions that will affect them taken solely by automated process.
  - sue for compensation if they suffer damage by any contravention of the legislation.
  - take action to rectify, block, erase or destroy inaccurate data.

    - request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened.
- AoG Inc will only process personal data in accordance with individuals' rights.

7) Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data.

- All functionaries are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties.
- AoG Inc. will ensure that all personal data is accessible only to those who have a valid reason for using it.

8) Ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

AoG Inc will not transfer data to such territories without the explicit consent of the individual.

This also applies to publishing information on the Internet - because transfer of data can include placing data on a website that can be accessed from outside the EEA - so AoG Inc will always seek the consent of clearly identifiable individuals before placing any personal data (including photographs) on its website.

If AoG Inc collects personal data in any form via its website(s), it will provide a clear and detailed privacy statement prominently on the website(s), and wherever else personal data is collected.

APPENDIX 2 - CONDITIONS FOR PROCESSING SPECIAL CATEGORY DATA

The conditions are listed in Article 9(2) of the GDPR:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection

and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
You need to read these alongside the Data Protection Act 2018, which adds more specific conditions and safeguards:

Schedule 1 Part 1 contains specific conditions for the various employment, health and research purposes under Articles 9(2)(b), (g), (i) and (j).

Schedule 1 Part 2 contains specific 'substantial public interest' conditions for Article 9(2)(h).
In some cases you must also have an 'appropriate policy document' in place to rely on these conditions.

Information taken from Information Commission Officer's website:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

APPENDIX 3 - COLLEGE

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:

Rob Ridler
Academic Liaison Officer
Assemblies of God Bible College
Retford Road
Mattersey
DN10 5HD
email: rridler@matterseyhall.com
Tel: 01777 817663 ext 18

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.

APPENDIX 4 - PURPOSES

ICO registration no longer includes registering "purposes". However this appendix is a comprehensive list of the purposes for which data may be held, and which can be used alongside an information asset register to check that AoG is within these listed purposes. The Information Controller's Office was asked about such an appendix and did not object to AoG doing this.

Accounts & Records

Purpose Description:
Keeping accounts related to any business or other activity carried on by the data controller, or deciding whether to accept any person as a customer or supplier, or keeping records of purchases, sales or other transactions for the purpose of ensuring that the requisite payments and deliveries are made or services provided by him or to him in respect of those transactions, or for the purpose of making financial or management forecasts to assist him in the conduct of any such business or activity

Data subjects are:
Staff including volunteers, agents, temporary and casual workers
Suppliers and Contractors
Complainants, correspondents and enquirers
Advisers, consultants and other professional experts
Business or other contacts
Employees of other organisations
Status Ministers and Churches
Retired Ministers

Advertising, Marketing & Public Relations

Purpose Description:
Advertising or marketing the business of the data controller, activity, goods or services and promoting public relations in connection with that business or activity, or those goods or services.

Data subjects are:
Members or supporters
Complainants, correspondents and enquirers
Advisers, consultants and other professional experts
Business or other contacts
Employees of other organisations
Status Ministers and Churches
Retired Ministers

Staff Administration

Purpose Description:
Appointments or removals, pay, discipline, superannuation, work management or other personnel matters in relation to the staff of the data controller.

Data subjects are:
Staff including volunteers, agents, temporary and casual workers

Relatives, guardians and associates of the data subject
Previous and prospective employers of the staff and referees

Administration of Membership Records

Purpose Description:
The administration of membership records.

Data subjects are:
Staff including volunteers, agents, temporary and casual workers
Members or supporters
Complainants, correspondents and enquirers
Donors and lenders
Status Ministers and Churches
Retired Ministers

Trading / Sharing in Personal Information

Purpose Description:
The sale, hire or exchange of personal information.

Data subjects are:
Staff including volunteers, agents, temporary and casual workers
Suppliers
Members or supporters
Complainants, correspondents and enquirers
Advisers, consultants and other professional experts
Donors and lenders
Status Ministers and Churches
Retired Ministers

Fundraising

Purpose Description:
Fundraising in support of the objectives of the data controller.

Data subjects are:
Staff including volunteers, agents, temporary and casual workers
Members or supporters
Complainants, correspondents and enquirers
Advisers, consultants and other professional experts
Donors and lenders
Status Ministers and Churches
Retired Ministers

Realising the Objectives of a Charitable Organisation or Voluntary Body

Purpose Description:
The provision of goods and services in order to realise the objectives of the charity or voluntary body.

Data subjects are:
Staff including volunteers, agents, temporary and casual workers
Customers and clients
Suppliers
Members or supporters
Complainants, correspondents and enquirers Relatives, guardians and associates of the data subject
Advisers, consultants and other professional experts
Business or other contacts
Employees of other organisations
Donors and lenders
Status Ministers and Churches
Retired Ministers

Accounting and Auditing

Purpose Description:
The provision of accounting and related services; the provision of an audit where such an audit is required by statute.

Data subjects are:
Staff including volunteers, agents, temporary and casual workers
Suppliers
Complainants, correspondents and enquirers
Advisers, consultants and other professional experts
Business or other contacts
Employees of other organisations
Status Ministers and Churches

Pastoral Care

Purpose Description:
The administration of pastoral care by a vicar or minister of religion.

Data subjects are:
Staff including volunteers, agents, temporary and casual workers
Members or supporters
Complainants, correspondents and enquirers
Advisers, consultants and other professional experts
Status Ministers and Churches
Retired Ministers

Other Commercial Services

Purpose Description:
The provision of consultancy and advisory services;
Provision of conference facilities (e.g. lecture halls, accommodation, catering etc.);
Other chargeable services (excluding tuition fees).

Data subjects are:
Staff including volunteers, agents, temporary and casual workers
Customers and clients Suppliers
Complainants, correspondents and enquirers
Relatives, guardians and associates of the data subject
Advisers, consultants and other professional experts
Students and pupils
Status Ministers and Churches
Retired Ministers
Courts / Tribunals
Customers and clients of the data controller for goods and services

Crime Prevention and Prosecution of Offenders

Purpose Description:
Crime prevention and detection and the apprehension and prosecution of offenders.
Data Controller's further description of Purpose:
Includes use of cctv (the use of closed-circuit television for the monitoring and collection of sound and/or visual images for the purpose of maintaining the security of premises, for preventing crime and for investigating crime)

Data subjects are:
Customers and clients
Offenders and suspected offenders
Members of the public.
Those inside, entering or in the immediate vicinity of the area under surveillance.