International Bible Training College (IBTI)
Impact the nations with your vocation

IBTI, Hook Place, Cuckfield Road
Burgess Hill, RH15 8RF
Tel: 01444-233173
Email: policies.data@ibti.org.uk
www.ibti.org.uk

DATA PROTECTION POLICY

Approved By:	**Board of Directors/Trustees**
Approval Date:	**30.04.2019**
Next review Date:	**19.05.2022**
Policy Holder:	**IBTC**

1. Introduction

In order to operate efficiently the International Bible Training College (IBTC)[1] needs to collect and use information about the current, past and prospective: staff (voluntary workers), students, sponsors, donors, supporters and others with whom we communicate and work.
IBTC regards the lawful and correct treatment of personal information as integral to its successful operation, and to maintaining the confidence of the people we work with. To this end we fully endorse and adhere to the principles of the **Data Protection Act 2018** which includes **General Data Protection Regulation (GDPR)** and is enforceable from May 2018, and has replaced the Data Protection Act 1998 as UK personal data protection Law.
This personal data protection policy addresses the incorporation into all activities of the College. The key seven principles and requirements of GDPR have been incorporated into the college's data protection policy, which addresses all activities of IBTC. In summary these state that personal data shall:

a) Be processed lawfully, fairly and in a transparent manner,
b) Be collected for specified, explicit and legitimate purposes,
c) Be adequate, relevant and limited to what is necessary,
d) Be accurate and where necessary kept up to date,
e) Be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed, and
f) Be processed in a manner that ensures appropriate security of the personal data.
g) Accountability is central to GDPR. Data controllers are responsible for compliance with the principles and must be able to demonstrate this to data subjects and the regulator.

Further details are given on the website of the Office of the Information Commissioner.

At IBTC the Principal's office is responsible for maintaining the College's registration and providing advice and guidance to assist in ensuring compliance with the General Data Protection Act 2018.

2. Purpose

The purpose of this policy is to ensure that everyone handling personal information at IBTC is fully aware of the requirements of the **Data Protection Act 2018** and complies with data protection procedures and that data subjects are aware of their rights under the GDPR.

[1] In all the following text International Bible Training College (IBTC) is referred to as IBTC. The college's trading name is IBTI.

3. Location of the policy

The college will ensure that the policy is available to all students and staff and will also be on the IBTC website: www.ibti.org.uk.

4. Legal Framework

IBTC will appraise itself of all legislative changes to ensure that it abides by its legal duties under current legislation. It will seek to develop best practice in all its activities and will review this policy annually.

5. Definitions and Scope

As a college we are required to take specific measures to ensure that all information ("personal data") held about living individuals, in either paper-based or computer format, is processed according to the seven Data Protection principles. This policy applies to current, past and prospective students, staff and others acting for or on behalf of the college or who are given access to college personal information. This policy covers all activities and processes of the college that uses personal information in whatever format.

5.1. Definitions of terms used in this policy

- **Data**

Data can be in computer or paper form and is any system that is a structured set of personal data and the records can be centralised, decentralised or dispersed. In effect this means all records of our: staff, student, sponsors, donors, supporters and others with whom we communicate.

- **Personal Data**

Personal data is information that relates to an individual who can be identified from that information, either by itself, or when used in conjunction with other information held by the college or other information likely to come into the possession of the college, to identify that person. Article 4 (1) of the GDPR defines personal data as: 'any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person'.[2]

It includes any expression of opinion about an individual and any indication of the intentions of the college in respect of the individual. It includes information stored in any medium: paper and electronic, text, image, audio and visual.

- **Sensitive Personal Data**

Sensitive personal data (or 'Special Category' data under the GDPR) means personal data consisting of information as to the Data Subject's -

- race;

[2] Information Commissioner's Office, "What is personal data?", [Internet], https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/, Accessed 24.08.2018.

- ethnic origin;
- nationality;
- political opinions;
- Mental Health (status, medical records conditions, to include disability);
- Physical Health (status, medical records conditions, to include disability)
- Dietary requirements;
- religious or philosophical beliefs;
- Counselling records;
- Pastoral records, including Extenuating Circumstances Forms
- Disciplinary records;
- Training records;
- trade union membership;
- biometric data (where this is used for identification purposes);

Sensitive personal data is personal data that could be used to discriminate against an individual or may cause them to be treated differently from others.

- **Processing**

'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

- **Data Subject**

Data subject means an individual who is the subject of personal data. This will refer to current, past and prospective staff, students, sponsors, donors, supporters and anyone else about whom we collect personal data. The Act does not count as a data subject an individual who has died or who cannot be identified or distinguished from others.

- **Data controller**

Data controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

In the case of the IBTC, the college is the data controller because it determines the purposes for which, and the manner in which, any personal data are processed or are going to be processed. IBTC is registered as a data controller by the Information Commissioner's Office and has nominated Data Protection Officer (DP Officer), Gordica Karanfilovska to operate in its name, who may be contacted directly to the office or via email policies.data@ibti.org.uk .

- **Data processor**

A data processor is any person other than an employee of the data controller who processes data on behalf of the data controller. For example, this could be a "Mail chimp" as a third-party email marketing service to deliver IBTC newsletters via their email platform.

- **Data users**

Data users are individual members of staff, students or others who process data on behalf of the IBTC. Personal data should always be processed according to the GDPR Principles.

- **Recipient**

Recipient, in relation to personal data, means any person to whom the data are disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of a data processor) to whom they are disclosed in the course of processing the data for the data controller, but does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law.

- **Third Party**

A third party is anybody other than the data subject, the data controller or any other person authorised to process personal data on behalf of the college or data processor. The expression third party does not include employees or agents of the data controller or data processor, who are treated as being part of the data controller or processor. Note that "third party" is different from "recipient", which effectively separates employees/agents of the data controller/processor from the data controller/processor itself.

6. Compliance

The co-operation of all concerned is essential for the success of this policy. However, ultimate responsibility for achieving the policy's objectives and for ensuring compliance with the relevant existing legislation is the responsibility of the Board of Directors/Trustees, the Principal and the Operations Director. Behavior or actions against the spirit and/or the letter of the law on which this policy is based will be considered serious disciplinary matters and may, in some cases, lead to dismissal.

7. Student privacy notice

This privacy notice explains how IBTC ("we", "our", "us") collects, uses and shares students personal data, and students rights in relation to the personal data we hold. This privacy notice concerns our processing of personal data of past, present and prospective students of IBTC ("you", "your") and is a separate document that must be read in conjunction with this policy and considered as a part of.

8. Permission forms

IBTC publishes various items which will include some personal data, e.g. internal telephone directory, event information, photos and information in marketing materials, etc.
It may be that in some circumstances an individual wishes their data processed for such reasons to be kept confidential or have a restricted college access only. Therefore it is IBTC policy to offer an opportunity to opt-out of the publication of such when collecting the information by using a permission forms. (**See in Appendix 3**).
This is a form used by IBTC to obtain the consent of the data subject for their personal data to be used for a particular purpose. A permission form needs to be referred at the point of the data collection or later, if the particular purpose of the data collection was not explicitly mentioned when the data was collected.

9. Procedures for data to be kept securely

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

The college will have in place appropriate security measures e.g. ensuring that:

a) all personal data is kept in lockable filing cabinets/cupboards with key controlled access;
b) personal data held electronically are password protected;
c) archiving personal data which is then kept securely (lockable cabinet and/or office with key-controlled access);
d) placing any PCs, external hard drives or cameras, etc. that show personal data in lockable cabinet and/or office with key-controlled access so that they are not visible except to authorised staff;
e) ensuring that PC screens are not left unattended without a password protected screensaver being used.
f) 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.

The college has a legal responsibility as an institution to operate within the terms of the above Act but each member of staff or student could also have a personal liability for any unauthorised disclosure they make. Disclosing information outside the terms of the college policy could result in disciplinary action. Data held by the college may only be disclosed to third parties in the following circumstances:

a) Internal requests

To college staff who require the information to carry out their normal duties within the scope of their agreed roles.

b) External requests

With the written authority of the student or staff, in accordance with the Student Privacy Notice.

c) Protection Statement(s) - is for one of the "crime and taxation purposes"

- When required by law or statutory instruction*
- When required to prevent or detect crime*
- The assessment or collection of any tax or duty or of any imposition of a similar nature.

As a general rule, the assumption now made is that information may only be given if there is a specific authority to do so, otherwise the concept of confidentiality should apply and the enquirers request declined.

Note: Requests made under headings with * must be referred to the DP Officer prior to any information being supplied to the party /authority who have made the request.

10. Data subject access request

Under the Data Protection Act 2018, individuals can ask to see the information about themselves that is held on a computer and in some paper records. If an individual wants to exercise this subject access right, they can do that by any means. IBTC will comply with any requests received in a letter, a standard email or verbally. However, IBTC has provided a Subject Access Request form (See **Appendix 1**) which you can obtain in hard copies from the DP Officer or downloading from IBTC's website and encourages you to use it when needed.

Where the request is manifestly unfounded or excessive IBTC may charge an appropriate fee (not exceeding £10) for the administrative costs of complying with the request.

If an individual requests further copies of their data following a request IBTC will base the fee on the administrative costs of providing further copies. Payment can be made: In cash, by cheque (Please make cheques payable to 'IBTC') or online.

A reply must be received within one month of receipt. IBTC can extend the time to respond by a further two months if the request is complex or IBTC has received a number of requests from the individual. In both cases IBTC will let the individual know within one month of receiving their request and explain why the extension is necessary.

IBTC can refuse to comply with a subject access request if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. In this case IBTC should inform the individual about:

a) the reasons IBTC is not taking action;
b) their right to make a complaint to the ICO or another supervisory authority; and
c) their ability to seek to enforce this right through a judicial remedy.

- **References as subject access request**

There is no obligation to disclose sensitive personal data in a reference. The DP Officer use his/her judgement as to whether the information is relevant, and therefore whether it is fair to disclose it.

Confidential references received by the IBTC are not exempt from data subject access requests. However, in deciding whether to disclose information, it is necessary also to consider the data privacy rights of the referee. Information contained in or about a confidential reference need not be provided if the release of the information would identify an individual referee unless:

- the referee has given his or her consent;
- the identity of the referee can be protected by anonymising the information;
- it is reasonable in all the circumstances to release the information without consent;

The College cannot refuse to disclose information from a confidential reference without giving a reason.

11. Specific Obligations regarding data protection policy

Training is provided at the IBTC induction for staff and additional guidance will be provided by the DP Officer whenever needed. Staff are expected to ensure they read the guidance available in this policy and are fully conversant with the requirements of this policy.

11.1. Processing personal data that is not registered is a criminal offence.

- Staff and students should ensure that any data which it is proposed to process are covered by the Privacy notice.
- In the first instance, queries should be raised with Line Managers (i.e. for students - their tutors) and then with the DP Officer. Issues that cannot be resolved on these levels should be referred to the Principal's office.

11.2. Any person for whom personal data is obtained should not be deceived or misled as to the purposes for which such data are held, used or disclosed.

- Staff and students must ensure that an indication of the purpose(s) should appear on any form used to collect data, and, where necessary, an explanation given as to why personal data is being collected.
- No unfair pressure should be used in order to obtain any personal data.

- Special care must be taken when collecting sensitive personal data. When proposing to process sensitive personal data confirmation must be obtained from the DP Officer in order to ascertain that the correct conditions for processing have been met.

11.3. All staff and students should observe strict control measures when handling all personal data, whether in computerised or paper based form, and whether it relates to staff, students or members of the general public.

- Failure of any member of staff to inform Data Protection Officer or college management of using a computerised database could result in disciplinary action.
- The holding of a college-related database (computerised or paper-based) outside the college (however temporarily) also falls within these restrictions.

11.4. Great care must be taken not to disclose personal data, either intentionally or accidentally, by:

- Only allowing authorised access to computers (eg. by not disclosing passwords).
- Switching off (or logging off) your computer when you're not using it.
- Keeping doors to rooms containing computers and/or personal papers locked when not in use.
- Preventing unauthorised information being obtained from a computer screen, computer printout or other paper-based material.
- Ensuring proper disposal of all paper containing personal data, including computer-based printouts.
- Not disclosing personal data over the telephone.
- Ensuring that the written authority of the data subject (person) is obtained when required.
- Only disclosing personal data where you are sure that it is being given to an individual/institution who/that is authorised to receive it.
- Not removing any college hardware or software from the college without prior authorisation.
- Not sending any data outside the 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 and without the specific written authority of the data subject (individual).
- Any circumstances where a decision is required on whether to disclose information should be referred in the first instance to the DP Officer, if it is needed, in consultation with the Principal's office.

11.5. It is recognised that on occasions it is necessary for members of staff to work from home.

In these circumstances, additional care must be taken with regard to the increased risk of unauthorised disclosure of personal data through theft, loss or access by family members or friends. Members of staff must recognise that the conditions enforced by the Data Protection Act 2018 within the college environment apply equally when working from home. Great care must be taken to ensure that any personal data removed from the college or accessed from management information sources (whether on laptop, USB memory key or in paper form) is kept secure from theft and viewing by unauthorised persons. If the data has been compromised the data breach reporting procedures will be implemented.

12. Data breach reporting procedures

The GDPR has introduced a mandatory requirement to notify the data regulator (the ICO) in the event of a breach of data that could have serious consequences for those whose data has been compromised. An

Information Security Incident can be defined as any event that poses a potential, suspected or actual threat to the security, confidentiality, integrity, or availability of IBTC Information.

A personal data breach can happen for a number of reasons, for example:

- Loss or theft of data or equipment on which data is stored, or through which it can be accessed
- Loss or theft of paper files
- Hacking attack
- Inappropriate access controls allowing unauthorised/unnecessary access to data
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood

12.1. Personal data security breach reporting process

a) Reporting an Incident

It is vital that as soon as a personal data breach is identified **or suspected** it is immediately reported to the DP Officer. In order to improve our understanding of the risks to data and address them before breaches occur we would also encourage individuals to report 'near misses' (i.e. incidents which have almost resulted in a data breach except for an intervention or 'luck'). Near misses should be reported using the same form and process as an actual breach highlighting clearly that the incident is a near miss.

The General Data Protection Regulation requires that all relevant breaches are reported to the supervisory authority (the Information Commissioner) '*without undue delay….., **not later than 72 hours** after having become aware of it'.*

As much information as is immediately available should be collated and the **Data Security Breach Report Form** (**Appendix 2**) should be completed and emailed to DP Officer (policies.data@ibti.org.uk) as soon as possible and within **twelve hours** of the breach being identified at the very latest.

The DP Officer will analyses the form, update the personal data breach and ascertain whether any immediate corrective/containment/escalation actions are required.

The **Personal Data Breach Log**[3] will be reviewed on a regular basis by the Board of Directors/Trustees who will determine whether any updates to Policy and Procedures are required, and co-ordinate any training and communications messages from the lessons learnt.

b) Investigating an Incident

Depending on the type and severity of the incident the DP Officer will assess whether a full investigation into the breach is required. Where required the DP Officer will appoint an appropriate investigation team who will complete a full breach report.

The investigation will:

- Establish the nature of the incident, the type and volume of data involved and the identity of the data subjects;

[3] Personal Data Breach Log is a file in which all the Data Security Breach Report Forms are kept.

- Consider the extent of a breach and the sensitivity of the data involved;
- Perform a risk assessment;
- Identify actions IBTC needs to take to contain the breach and recover information;
- Assess the ongoing risk and actions required prevent a recurrence of the incident.

13. Reporting breach to the Information Commissioner or data subject

The Data Protection Officer and the investigation team if it has been formed, will co-ordinate breach reporting to the Information Commissioner within 72 hours of becoming aware of a relevant breach. They will also evaluate whether the breach is 'likely to result in a high risk to the rights and freedoms' of the data subject. If this is determined to be the case the incident it will also be reportable to the data subjects without undue delay. Any such report will be coordinated by the DP Officer, assistance will be required from all members of staff and should be made available on demand.

14. Data protection complaints procedure

IBTC aims to comply fully with its obligations under the Act. If you have any questions or concerns regarding IBTC's management of personal data, including your right to access data about yourself, or if you feel IBTC holds inaccurate information about you, please contact IBTC's DP Officer (details above). If you feel that your questions or concerns have not been dealt with adequately or that a subject access request you have made to IBTC has not been fulfilled you can use IBTC's General Complaints Policy. If you are still dissatisfied, you have the right to contact the Information Commissioner's Office, the independent body overseeing compliance with the Act: https://ico.org.uk/

15. Mechanisms for Feedback

Constructive comment for the continued improvement of this policy is welcomed and should be forwarded to the IBTC's Data Protection Officer at policies.data@ibti.org.uk.

16. References[4] and further information

- The International Bible Training College: https://www.ibti.org.uk/
- Data Protection Act 2018: http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
- Information Commissioner's Office: www.ico.org.uk

[4] In addition to taking information from the Data Protection Act 1998 and Information Commissioner's Office, the IBTC has sourced material from the following websites: Sutton College, *Missions and Policies,* [Internet], https://www.suttoncollege.ac.uk/wp-content/uploads/2011/06/Data-Protection-Policy-Sept-2015.pdf, and University of Reading, *Data Protection*, [Internet], http://www.reading.ac.uk/internal/imps/DataProtection/imps-d-p-glossary.aspx#SAR, accessed 20 March 2017.

APPENDIX 1:

Subject Access Request

"Subject access" is the right of an individual to access personal data relating to him/her which is held by the International Bible Training College (IBTI)[5]. Please complete and return this form to the college Academics Manager and Data Protection Officer, Gordica Karanfilovska directly to the office or via email policies.data@ibti.org.uk . Examination scripts are exempt from subject access rights.

APPLICANT DETAILS	
Name and Surname	
Position (student or staff)	
Postal / email address*	
Home /Mobile number**	
Please write the dates: the years you started and you graduated at IBTC. (if applicable)	
*If you would like your information electronically please provide an email address. **If you do not wish for us to contact you by phone please leave blank.	
THE PERSONAL DATA YOU REQUIRE	
Please specify which personal data you would like access to by identifying any specific or types of documents. Examples are 'Transcript', 'Staff file', 'Student file' or 'Mentoring file'. *(please continue on additional sheets, if necessary)*	

Signature:		Date:	

Please provide evidence of your identity, e.g. a driving license or passport or give a phone call personally. You will receive an answer within max. one month of receipt. Data protection laws allow for an extension of up to 2 months for responding to very complex requests. We may also refuse requests that are deemed manifestly unfounded or excessive and reserve the right to charge a fee. In such cases the reason for refusal, delay, or any fees payable will be explained in writing.

[5] In all the following text International Bible Training College (IBTC) is referred to as IBTC. The college's trading name is IBTI.

APPENDIX 2:

DATA SECURITY BREACH REPORT FORM

This form should be completed in the event of an actual, suspected or potential information security incident.

The effective management of information security incidents is required in order to ensure we meet our obligations under the GDPR law, to maintain the security and integrity of the data we hold, as well as being necessary to ensure mitigating and remedial measures can be put in place promptly.

This form can be completed by any member of staff (students should refer any incidents to a member of staff) that becomes, or is made, aware of an Information security incident. This form should be completed as soon as possible, without undue delay, and submitted to the college's address or return to directly to the office or via email: policies.data@ibti.org.uk. To ensure risks of further compromise of data are minimised, please treat the information contained within this form as strictly confidential unless advised otherwise.

1. REPORTING PERSONS' DETAILS	
Name	
Email	
Contact Number	
2. INCIDENT DETAILS	
Date of Incident	Click here to enter a date.
Type of Incident	Choose an item.
Breach effect	
Number of data subjects affected	
Number of personal data records affected	
Does the data at risk include personal data (for example names, addresses, emails)	Choose an item.
Summary of Incident. Please provide details.	Click here to enter text.

3. IBTC OFFICE USE ONLY[6]		
Data of Breach Report Received	Click here to enter a date.	
Action Taken	Choose an item.	
Actions taken. Have any mitigating measures already taken to resolve or remedy the incident and/or prevent future occurrences?	Choose an item.	Click here to enter text.
Date actioned/referred	Click here to enter a date.	
DP Officer Signature		

[6] **Copies of this form to be retained by Data Protection Officer for 3 years from the date of incident resolution.**

APPENDIX 3:

PERMISSION FORM
TO DISCLOSE PERSONAL AND SPECIAL CATEGORY DATA[7]

(To be completed by the data subject).

	The information that you supply via this form will be entered into a filing system and will only be accessed by authorised persons of the IBTC. The information will be retained by the IBTC and will only be used for the purpose of (a) processing your Subject Access Request, and (b) summary information for statistical and audit purposes. By supplying such information you consent to the IBTC storing the information for the stated purposes. The information is held by the IBTC in accordance with the provisions of the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) law.

The college collects, holds and processes personal data relating to its staff, students, sponsors, donors, supporters and anyone else about whom we collect personal data, in accordance with the Data Protection Act 2018 and the GDPR law. The information that is provided is used for the administration, marketing, planning and management of the work of the college, student education and training and administering of student and college funding.

To comply with the Data Protection Act (2018) and the GDPR law we must tell you how we use personal information, collected by paper, electronically, telephone calls, surveys, audio, video and on-line applications on the web data and ask for your permission. By signing this form you are providing your permission for us to process your data for the purposes stated below as well as in the student privacy notice document. (See Appendix 4)

The college may be legally required to pass on some of this data to various agencies, government departments and local authorities. In this case the information is used for the exercise of functions of these government departments and to meet statutory requirements. IBTC may share some information with other organisations, charities and churches with which it collaborates and where necessary regarding a student's placement and outreaches. The information that students provide may also be shared with awarding bodies, other organisations for education, training, volunteer work, employment and wellbeing-related purposes according to IBTI's legitimate interest.. If requested, information may be shared with the Police in relation to a crime.

Further information about the use of, and access to, your personal data and details of organisations with which we may share data, you can get from the Data Protection Officer at IBTC, Gordica Karanfilovska, personally, via email policies.data@ibti.org.uk. All information provided will be dealt with in accordance with the college Data Protection policy. Personal information will not be passed on to other organisations for their own marketing or sales purposes.

The legal basis of IBTC processing your personal data is based on consent and IBTC's legitimate interest. For your benefit we keep your academic record and relevant personal data related to your time as a student here with us. **The retention period for these records should reflect the need to fulfil this obligation over long periods of time, perhaps for the lifetime of the student (permanent retention).** Your personal data that IBTC uses to communicate with you will be kept until you withdraw your consent. Under GDPR you have the following rights as individuals: the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object and rights in relation to automated decision making and profiling. If you feel any these have been not respected then feel free to contact the IBTC Data protection officer, personally, via email

[7] Special category data is personal data which the GDPR says is more sensitive, and so needs more protection. They are: the racial or ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation data.

or you can contact directly the Information Commissioner's Office.
The data that we collect are: personal details (name, address, date of birth), phone numbers, email addresses, gender, photographs, academic marks, appraisals, references, disciplinary information, health and disability information, ethnicity data, dietary requirements, information regarding your skills, hobbies and interests, any other legitimate personal data relating to academic and pastoral support.

Primary purposes for processing student information are:

- To enable effective communications with you.
- To support your training, health, safety and welfare / pastoral care requirements.
- To administer the financial aspects of your relationship with us and any funders, e.g. payment of students' lodging, provision of funds.
- Security and crime prevention.
- To manage your use of facilities and participation in events (e.g. computing, including email accounts and internet access, libraries, accommodation, functions, graduation).
- To facilitate your education, record the details of your studies (registration, progress monitoring, including any placements with external organisations, calculation and publication of assessments, provision of references).
- Administration of applications (receiving and processing applications, compilation of statistics, assessments of applications).
- To operate security, disciplinary, complaint and quality assurance processes and arrangements.
- To produce statistics and research for internal and statutory reporting purposes.
- To monitor our responsibilities under equalities legislation.

This is not an exhaustive list but sets out the primary reasons why IBTC handles student personal data.

1: Please provide the following information to confirm your identity	
Your full name	
Your date of birth	
Your current home telephone and mobile number	
Your current e-mail address	
Your date of starting your study at the IBTC	
Your home address	
3: To be completed by an applicant	
I certify that I am the data subject and the information given above is correct to the best of my knowledge and belief. I am aware that the IBTC will create and maintain computer (photo, audio and video) and paper records on me, both during my course and after I leave IBTC. I understand and I consent that IBTC will process my personal and special category data strictly in accordance with the Data Protection Act 2018 and GDPR law both internally within IBTC and externally to other awarding bodies or governmental departments to protect my or another person's vital interests and also in an emergency my data may be disclosed to others for medical reasons.	

- The data collected by IBTC will be used for the purpose of IT administration within IBTC and will not be disclosed to any external sources without your express written consent.

  I agree: ☐ I disagree: ☐

- The data collected by IBTC, photos, audio and video records during my studies and after graduation may be used for the purposes of marketing and promoting IBTC. The data will not be disclosed to any organization not associated with IBTC.

  I agree: ☐ I disagree: ☐

- Contact details (e.g. email address, phone number) collected by IBTC will only be used for the purpose of students' and IBTC course administration, but may be disclosed to:

  a) Appropriate bodies/organizations associated with IBTC. I agree: ☐ I disagree: ☐
  b) Former IBTC students. I agree: ☐ I disagree: ☐

- IBTC may share your personal information with other organisations, charities and churches with which it collaborates and where necessary regarding a student's placement and outreaches.

  I agree: ☐ I disagree: ☐

- You may be contacted after you have completed your programme at IBTC or your volunteer work for further collaboration with IBTC and its projects. Please, indicate below if you do not want to be contacted.

  ☐ No, thank you, I don't wish to receive any communication from IBTC.

  ☐ Yes, I want to stay connected by receiving communication from IBTC via (choose one or more of the options below by putting X)

  - Email - I want: ☐ I don't want: ☐
  - Phone - I want: ☐ I don't want: ☐
  - Post - I want: ☐ I don't want: ☐
  - Text - I want: ☐ I don't want: ☐

- Please write down in which other situation that is not mentioned above you don't want your personal or special category data to be disclosed:

_____
_____
_____

I hereby give my consent to the disclosure of my personal and special category data for the above purposes named in this document and Student privacy notice[8].

After giving this consent you can change your mind at any time about how we communicate with you in the future if you call us or send an email to policies.data@ibti.org.uk.

Signature: _____ Date: _____

[8] For more detailed information about the use of your data, please see the Student privacy notice that you find in the IBTC Library in the IBTC Policies file.

APPENDIX 4:

STUDENT PRIVACY NOTICE

This privacy notice explains how International Bible Training College (IBTC)[9] ("we", "our", "us") collects, uses and shares your personal data, and your rights in relation to the personal data we hold. This privacy notice concerns our processing of personal data of past, present and prospective students of IBTC ("you", "your").

IBTC is the data controller of your personal data and is subject to the **Data Protection Act 2018** ("DPA") which includes **General Data Protection Regulation (GDPR)**

1. How we collect your information

We may collect your personal data in a number of ways, for example:

a) from the information you provide us with when you interact with us before joining a course, for example when you express your interest in studying at IBTC;
b) when you apply to study at IBTC and complete enrolment forms;
c) when you communicate with us by telephone, email or via our website, for example in order to make enquiries or raise concerns;
d) in various other ways as you interact with us during your time as a student at IBTC, for the various purposes set out below;

2. The types of information we collect

The college collects, holds and processes personal data relating to its students about whom we collect personal data, in accordance with the **Data Protection Act 2018** which includes **General Data Protection Regulation (GDPR) and** the **College Data Protection policy**. The information that the students provide is used for the administration, planning and management of the work of the college, student education and training and administering of student and college funding. Personal information will not be passed on to other organisations for their own marketing or sales purposes.

You may be contacted after you have completed your programme at IBTC for further collaboration with IBTC and its projects. You can indicate on your permission form if you do not want to be contacted. Further information about the use of, and access to, your personal data and details of organisations with which we may share data, you can get from the Data protection officer, Gordica Karanfilovska at IBTC.

We may collect the following types of personal data about you:

a) Personal details and contact information (gender, name, address, date of birth and passport number, phone numbers, email addresses
b) Information relating to your education and employment history, the courses you have completed, dates of study and examination results from your studies at IBTC. Also your examination grades and other information in your individual learner file.
c) Information about your family or personal circumstances, and both vocational and extracurricular interests (e.g. skills, hobbies and interests).

[9] In all the following text International Bible Training College (IBTC) is referred to as IBTC. The college's trading name is IBTI.

d) Any other legitimate personal data relating to academic and pastoral support, for example to provide you with appropriate pastoral care;
e) Counselling records;
f) Sensitive personal data and information about criminal convictions and offences, including:

- information concerning your health and medical conditions (e.g. disability and dietary needs);
- certain criminal offence or conviction information
- information about your racial or ethnic origin; religion or similar beliefs; and
- financial information and bank details

g) photographs
h) appraisals
i) references
j) disciplinary information

3. How we use information about our students

The purposes for which we may use personal data (including sensitive personal data) we collect during a student's association with us include:

a) recruitment and enrolment;
b) academic matters, including:
- the provision of our core teaching, learning and assessment services (e.g. registration, assessment, attendance, managing progress, certification, placement and any other activity while studying at IBTC);
- maintaining student records;
- assessing your eligibility for placement, further ministry in churches or other Christian organisations;

c) non-academic matters in support of our core services, including:
- providing student support services (e.g. Information, mentoring, counselling and guidance);
- monitoring equal opportunities;
- safeguarding and promoting the welfare of students;
- ensuring students' safety and security;
- managing the use of social media;
- administering the financial aspects of your relationship with us and any funders, e.g. payment of students' lodging, provision of funds.

d) other administrative purposes, including:
- promoting our college;
- dealing with grievances and disciplinary actions;
- dealing with complaints and enquiries.

This is not an exhaustive list but sets out the primary reasons the IBTC handles student personal data.

4. The basis for processing your information and how we use it.

We may process your personal data because it is necessary:

a) for the performance of your application;
b) for us to carry out legally required duties;
c) for us to carry out our legitimate interests;
d) for us to protect your interests;

We may also use your personal data for the following:

a) to interact with you before you are enrolled as a student, as part of the enrolment process (e.g. to send you a brochure or answer enquiries about our courses);
b) once you have enrolled, to provide you with the college regulations, code of conduct, training, fees, etc. as set out in our student handbook;
c) to deal with any concerns or feedback you may have;
d) to monitor and evaluate the performance and effectiveness of IBTC, including by training of our staff or monitoring yours and their performance.
e) to maintain and improve the academic, financial, estate and human resource management of IBTC.
f) to promote equality and diversity throughout IBTC.
g) to seek advice on our rights and obligations, such as where we require our own legal advice;
h) recovering money you owe to us;
i) for fundraising purposes;
j) to meet our compliance and regulatory obligations, such as safeguarding requirements;
k) for the prevention and detection of crime;
l) in order to assist with investigations (including criminal investigations) carried out by the police and other competent authorities;
m) to protect your or another person's vital interests (safeguarding or Prevent duties)

We may also process your personal data for other reasons where we have your specific or, where necessary, explicit consent to do so.

5. Sharing information with others

The college may be legally required to pass on some of this data to various agencies, government departments and local authorities. In this case the information is used for the exercise of functions of these government departments and to meet statutory requirements.

IBTC may share some information with other organisations, charities and churches with which it collaborates and where necessary regarding a student's placement and outreaches according to their consent and IBTC's legitimate interest as a lawful basis for processing personal data. The information that students provide may also be shared with awarding bodies, other organisations for education, training, volunteer work, employment and wellbeing-related purposes according to IBTC's legitimate interest as a lawful basis. If requested, information may be shared with the Police in relation to a crime.

We may also share your personal data with other third parties including professional and regulatory bodies (e.g examination boards) in relation to the confirmation of qualifications, professional registration).

6. How long should we keep student records?

After you leave IBTC as a graduate student certain parts of your data may be retained as a permanent

archival record for research purposes and to confirm your award and period of study. If you are not successful in your application or you reject the offer to study at IBTC, the data which you have provided as part of your application will be removed from our record.

In general the retention of student records falls into three broad categories: **short, medium and permanent.**

It is the nature of the activities which give rise to these categories, and having a better understanding and appreciation of what these are, will help to identify which category individual documents will fall into. Once you have determined the category it is the record owner's responsibility to determine the exact length of time these records should be kept. The IBTC Retention Schedule lists the minimum amount of time the records should be kept. If IBTC wishes to keep records for longer they should make a noted reference within their own records keeping documentation explaining the reasons why.

a. **Short Term Retention Records** relating to the student as an individual and consumer of IBTC services are relatively short term and should be retained for a short finite period once the student leaves IBTC. This period should be shorter than for records relating to the wider arrangements. E.g. applicant records for unsuccessful applications relate to individuals who have not entered into a contract with IBTC and should therefore be included within this short-term category for retention.

b. **Medium Term Retention** - The contractual relationship between the institution and the student is subject to the same statutory limitations on action as any other contract. The current limitation period as defined by the Limitation Act 1980[10] is 6 years. The date at which the student leaves that programme of study normally provides the retention 'trigger' for when this retention period begins.

c. **Permanent Retention** - IBTC has an obligation, during a student's working life, to provide factual information on what they have studied and achieved, i.e. a transcript, students' applications, and students' register. The retention period for these records should reflect the need to fulfil this obligation over long periods of time and therefore will have permanent retention period.

d. Requirements under the Data Protection Act 2018 - The Data Protection Act does not specify a time period for retaining personal information rather it states that personal data should 'not be kept for longer than is necessary'. It is therefore for the college to decide what length of time is considered 'necessary'.

7. Keeping personal data up to date

The Data Protection laws require us to take reasonable steps to ensure that any personal data we process is accurate and up-to-date. Applicants and students are responsible for informing us of any changes to the personal data that they have supplied during the course of their application and enrolment. Enrolled students can update their details by contacting the Data Protection Officer via email policies.data@ibti.org.uk or IBTC Administrator Phillida Bennett via email admin@ibti.org.uk .

8. Your rights

[10] Legislation.gov.uk, Limitation Act 1980, CHAPTER 58, Arrangement of sections, Part i, ordinary time limits for different classes of action, [internet], https://www.legislation.gov.uk/ukpga/1980/58/pdfs/ukpga_19800058_en.pdf, Accessed, 01.10.2018.

Under GDPR you have the following rights:

a) to obtain access to, and copies of, the personal data that we hold about you;
b) to require that we cease processing your personal data if the processing is causing you damage or distress;
c) to require us not to send you marketing communications;
d) to require us to correct the personal data we hold about you if it is incorrect;
e) to require us to erase your personal data (excluding some of the academic data that has **permanent retention period).**
f) to require us to restrict our data processing activities (and, where our processing is based on your consent, you may withdraw that consent, without affecting the lawfulness of our processing based on consent before its withdrawal)
g) to receive from us the personal data we hold about you which you have provided to us, in a reasonable format specified by you, including for the purpose of you transmitting that personal data to another data controller.
h) to object, on grounds relating to your particular situation, to any of our particular processing activities where you feel this has a disproportionate impact on your rights.

Please note that the above rights are not absolute, and we may be entitled to refuse requests where exceptions apply.

If you have given your consent and you wish to withdraw it, please contact our Data Protection Officer using the contact details set out below. Please note that where our processing of your personal data relies on your consent and where you then withdraw that consent, we may not be able to provide all or some aspects of our services to you and/or it may affect the provision of those services.

9. Requesting Information

As noted above, you have the right to access information held about you. Your right of access can be exercised at any time by contacting the Data Protection Officer.

10. Contact us

If you have any queries about this privacy notice or how we process your personal data, or to request access to the personal data that we hold about you, you may contact our Data Protection Officer, Gordica Karanfilovska by email: policies.data@ibti.org.uk, or by phone on+44(0)1444 248 383.

If you are not satisfied with how we are processing your personal data, you can make a complaint to the Information Commissioner's Office. You can find out more about your rights under data protection legislation from the Information Commissioner's Office website available at: www.ico.org.uk.

11. References and further information

- International Bible Training College: https://www.ibti.org.uk/
- Data Protection Act 2018: http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
- Information Commissioner's Office: www.ico.org.uk