allnations
training for mission

DATA PROTECTION POLICY 2021-22

Document Title		
DATA PROTECTION POLICY		
Document Author and Department:	**Responsible Person and Department:**	
Kathryn Edmonds, BA	Principal/CEO, Senior Leadership Team	
Approving Body:	**Date of Approval:**	
Board of Trustees	23rd February 2022	
Date coming into force:	**Review Date:**	
23rd February 2022	Annually	4
EITHER For Public Access? **Tick as appropriate**	**OR** For Internal Access only? **Tick as appropriate**	
YES ✓	**YES**	

Summary/Description:

This document sets out the principles of data protection compliance at All Nations Christian College to ensure that it processes all data fairly and complies with the Data Protection Act 2018. This document should also be read in conjunction with the relevant privacy notice, which are available on the College website. Students should also ensure that they read the **HESA Student Collection Notice**.

This document has been adapted from a policy document by The Open University, with grateful acknowledgment.

Reviewed December 2021: Amended section 3.4 – change of post holder
Feb 2022: Amended *Roles Responsibilities, Policy Approval and Review* section to bring it into line with all other College policies

ALL NATIONS CHRISTIAN COLLEGE

To train and equip men and women for effective participation in God's mission
to His multicultural world.

DATA PROTECTION POLICY

1. CONTENTS OF POLICY

2. POLICY STATEMENT

2.1. All Nations Christian College is committed to ensuring that it processes personal data only in a manner which respects the rights of individuals and in compliance with its legal obligations. Personal data must be handled in accordance with the data-protection principles, as set out in the Data Protection Act 2018 (DPA) and must be protected from unlawful or unauthorised disclosures, loss, damage or destruction.

2.2. To achieve this aim, we shall process and store all personal data in accordance with this policy. Failure to comply with data protection law and to provide appropriate protection for personal data may expose the College to financial penalties, payment of damages and damage to its reputation. Personal data is entrusted to the College for specified and lawful purposes and a failure to comply with the data protection law also breaches their trust.

3. DEFINITIONS

3.1. **Data** is information which is stored electronically, on a computer or other media (e.g. photograph or video) or in paper-based filing systems.

3.2. **Personal data** means any information relating to an identified or identifiable living person; this is someone who can be identified, directly or indirectly, including by reference to an identification number (e.g. student number) or by another identifying factor (e.g. name, date of birth etc).

3.3. **The Data Controller** is All Nations Christian College. All Nations Christian College Limited is a registered charity (no. 311028) and a company limited by guarantee, registered in England (no. 990054). The College has a wholly owned trading subsidiary: All Nations Trading Limited, a registered company (no. 1189164). Both companies have a registered address of: Easneye, Ware, Hertfordshire, SG12 8LX. The College is registered under the DPA for data protection purposes (reg. no. Z6320083).

3.4. **The Data Protection Officer** is the Head of Operations who can be contacted at info@allnations.ac.uk

3.5. **Information Commissioner's Office (ICO)** is the supervisory authority empowered by the DPA to police and enforce the relevant data protection legislation. For more information see https://ico.org.uk

3.6. **Data Subjects** are those whose personal data is processed by the College and who have rights under the DPA regarding the processing of that data.

3.7. **Data Users** are those employees of the College whose work involves processing personal data for the College.

3.8. **Processing** covers everything which might be done to personal data from its creation to its destruction, including collection, recording, organising, storage, adaptation or alteration, retrieval, consultation, use, disclosure, blocking, erasure or destruction.

3.9. **Special Category Data** (also known as Sensitive Personal data) includes information about such things as, but not exclusively, a person's gender, sexual orientation racial or ethnic origin, religious or similar beliefs, or physical or mental health or condition.

3.10. **Privacy Notice** is a public statement of how a Data Controller applies data protection principles to processing personal data. It should be a clear and concise document that is accessible by individuals.

4. SCOPE

This policy document applies to the storage and processing of all personal data held by All Nations Christian College. It covers all personal data held by the College, including the personal data of past and present: enquirers, applicants, students, alumni, employees, voluntary workers, volunteers, Missionaries-in-Residence, Trustees, hirers, guests, conference/course delegates, external library users and supporters; this list is not exhaustive. This policy does not form part of any employee's contract of employment.

5. LEGISLATIVE FRAMEWORK

This policy has been developed in accordance with the following regulations, policies and procedures. This list is not exhaustive:

- Data Protection Act 2018
- Equal Opportunities Act 2010
- The General Data Protection Regulation (GDPR)
- The Privacy and Electronic Communications Regulations (EC Directive) (PECR)
- All Nations Christian College Policy and Procedures
- All Nations Equal Opportunities Policy
- QAA UK Quality Code for Higher Education – Part C: Principle 3 *'Information should be available and retrievable where intended audiences and information users can reasonably expect to find it. The format and delivery of information should take account of the access requirements of a diverse audience.'*
- Open University Handbook for Validated Awards

6. POLICY PRINCIPLES

Personal data must:

i. be processed fairly, lawfully and in a transparent manner;
ii. be collected and processed for specified, explicit and limited purposes and not processed in any way that is incompatible with those purposes;
iii. be collected proportionately and only when relevant i.e. it must be adequate and not excessive and sufficient information should be obtained to avoid confusing the identities of different data subjects and hence to avoid unlawful or unauthorised disclosures of personal data;
iv. be accurate and where necessary, kept up to date; all reasonable steps must be taken to ensure that personal data is inaccurate, is erased or rectified without delay; personal data should be checked for accuracy at the point of collection and at appropriate intervals afterwards;
v. not be kept in a form which permits identification of data subjects for longer than is necessary for the purpose;
vi. be processed in accordance with data subjects' rights as set out in our Privacy notices;
vii. be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;
viii. be accessed internally by data users on a 'need-to-know' basis and only for the purpose for which it was collected;
ix. never be unlawfully disclosed to any other person or organisation unless legally obliged to do so or with prior written permission from the data subject;
x. not be transferred to people or organisations situated in countries outside the European Economic Area unless the country offers adequate data protection for the rights of data subjects or one of the permitted exceptions in the DPA applies;
xi. be made available to the data subject within 30 days of the Data Protection Officer receiving a request;
xii. be destroyed in a timely manner and in accordance with the College Data Disposal Schedule.

7. FAIR AND LAWFUL PROCESSING

7.1. The College will ensure that the process of personal data is done fairly and without adversely affecting the rights of the data subject.

7.2. For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds permitted by the DPA. These include processing:

i. with the data subject's consent;
ii. where necessary for the performance of a contract with the data subject;
iii. where necessary for All Nation's compliance with a legal obligation (e.g. reporting requirements to the College validating partner or regulators. Among other things, this includes the legal obligation to share data subjects' information with the Higher Education Statistics Agency who produce statistical data. This data is then shared by these public bodies to fulfil their public functions);
iv. for All Nation's legitimate interest or the legitimate interests of the party to whom the data is disclosed, provided there is no unwarranted breach of the data subject's rights and freedoms;
v. that is in the vital interest of the data subject (i.e. to protect their life).

8. CONSENT

8.1. Consent must be freely given, specific, informed and an unambiguous indication of the data subject's wishes. It must be a statement or clear affirmative action which signifies agreement to the processing of personal data relating to the data subject.

8.2. Where the College relies on the consent of the data subject for the processing of their data, data subjects must be informed of their right to withdraw consent at any time and the College's obligation to honour that request.

8.3. Under certain circumstances (e.g. when communicating via the phone) consent may be given verbally but a record must be kept of the information given at that time to the data subject to prove that their consent was informed.

9. DIRECT MARKETING

9.1. 'Direct marketing' means the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals. This includes contact made by organisations to individuals solely for the purpose of promoting their aims and the advertising need not be of a commercial product, nor need anything be offered for sale.

9.2. The College will adhere to the rules set out in the GDPR, the Privacy and Electronic Communication Regulations and any laws which may amend or replace the rules governing direct marketing when we make contact with data subjects, where that contact is made by (but not limited to) post, email, text message, social media messaging, telephone (both live and recorded calls) and fax. Stricter rules apply to marketing by email and other electronic means including text messaging, social media messaging, fax and automated telephone calls.

9.3. Any direct marketing material that the College sends will identify us as the sender and will describe how an individual can object to receiving similar communications in the future.

10. SPECIAL CATEGORY OR SENSITIVE PERSONAL DATA

10.1. See definition in section 3 above.

10.2. All special category data usually requires the specific, informed, written consent of the data subject. Clear information must be provided to data subjects to indicate why the information is being sought (for example to assess what, if any, reasonable adjustments must be made and to implement those adjustments) together with all the other information provided in a privacy notice (see the next section).

11. DISCLOSURE

11.1. If the College shares the personal data it holds with a third party, this must be disclosed to the relevant data subjects in their privacy notice, with reasons given for the disclosure.

11.2. Personal data must not be disclosed:

i. in response to a telephone enquirer unless the caller's identity can be verified as being that of the data subject.

ii. to a third party, unless the requester can demonstrate that he/she has a statutory power to obtain the data in question, is acting on the data subject's behalf or with their written permission (already provided) or that an exemption applies to render the

disclosure lawful or, in the absence of the relevant court order, without clear written assurances that the personal data falls within the crime-prevention/detection exemption.

12. DATA SECURITY

12.1. The College will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data, from collection to destruction.

12.2. Personal data will only be transferred to a data processor (i.e. a company or person processing personal data not in its own right but on behalf of the College) if it is subject to a written contract in which the data processor maintains the security requirements which apply to the College and which otherwise complies with the DPA.

12.3. The level of security will be appropriate to risks inherent in the processing of the personal data, in particular the risks and consequences of accidental or unlawful processing or unlawful destruction, loss, alteration, unauthorised disclosure of or access to the personal data processed. Security measures may include the following:

i. **Pseudonymisation**. Where appropriate, ensuring personal data is not attributable to individual persons without the use of additional information which is kept separate, secure and restricted (e.g. using student I.D numbers rather than names).

ii. **Secure lockable desks and cupboards or rooms**. Unoccupied rooms and/or desks and cupboards must be kept locked if they hold confidential information of any kind.

iii. **Methods of disposal**. Paper documents must be shredded and digital storage devices should be physically destroyed when they are no longer required.

iv. **Equipment.** Data users must ensure that individual monitors do not show confidential information, such as sensitive personal data, to passers-by and that they switch off their computer screens when they are left unattended. Computer files containing personal data must be password protected and be stored on computer drives accessible by data users with allocated accounts and passwords in order to restrict access to personal data to only those who need such access. Further, differing levels of access will be granted to data users, depending on the need for that data user to have access.

v. **Personal Devices.** Where confidential data is stored on personal devices, such as mobile phones, tablets or home computers, it is the responsibility of the owners to ensure these devices are encrypted and stored safely to minimise the risk of unauthorised access. College staff must comply with the security measures outlined in the Personal Portable Devices Policy.

vi. **Confidentiality.** Staff and any contractors are subject to a legally binding duty of confidentiality regarding personal data.

13. TRANSFERRING PERSONAL DATA OUTSIDE THE EEA

13.1. The College must only transfer personal data outside the EEA if there is adequate protection for the rights of data subjects in accordance with the DPA. This could be because the country is included in a list of those regarded by the EU Commission as providing adequate protection or the transfer is subject to standard contractual clauses approved by the EU Commission. Data can be transferred outside the EEA with the subject's consent. This would cover verifications of award to third parties for overseas employment, visas and application of overseas educational institutions.

13.2. As of 20 July 2018, the GDPR became directly applicable to the EEA and three of the four EFTA States (Liechtenstein, Norway and Iceland). By mid-2019, Switzerland is expected to

produce a major revision to its Federal Data Protection Act) and Data Protection Ordinance Data. The current Swiss legislation regarding the transfer of personal data is derived from the EU model clauses.

14. DATA RETENTION

14.1. Data must only be kept for as long as necessary to fulfil its stated purpose, unless the College is legally required to retain it for longer.

14.2. Data must be destroyed in a manner which will not risk a data breach.

14.3. Data must be destroyed in a timely manner and in accordance with the College Data Disposal Schedule.

15. DATA BREACHES

15.1. Breaches of this Data Protection Policy must be reported immediately to the College Data Protection Officer.

15.2. To demonstrate the College's compliance with GDPR, the College will keep records of all data breaches that may occur. The records will be kept by the Data Protection Officer and identify:

i. the facts relating to the personal data breach;
ii. its effects; and
iii. any remedial action taken.

15.3. Under the DPA, reporting breaches to the Information Commissioner/Supervisory Authority and in some circumstances to the data subject is mandatory and consequently it is important that reports are made to the Data Protection Officer without delay.

15.4. All data users have the right to complain about any processing concerns they may have. They may complain to the College Data Protection Officer at info@llnations.ac.uk and, should they consider the College to have breached data protection legislation to the ICO (Information Commissioner's Office) at https://ico.org.uk/make-a-complaint/

16. DATA PROTECTION BY DESIGN AND DEFAULT

The College will put in place appropriate technical and organisational measures to ensure that all personal data is processed in accordance with the data protection principles outlined in paragraph 6 and thereby safeguard the rights of data subjects. In particular, and not exclusively, computer and paper filing systems will be organised in a way that will:

i. minimise the risk of a data breach
ii. simplify file deletion
iii. enable a particular data subject's data to be traced should a data request be made
iv. pseudonymisation will be utilised wherever practicable
v. data protection will be a priority when considering the implementation of new computer systems, software and processes e.g. new courses will be designed from the outset with data protection and erasure in mind
vi. Data users will be given regular training to keep data protection at the forefront of all they do.

17. DATA PROTECTION IMPACT ASSESSMENTS

17.1. The College will consider carrying out a Data Protection Impact Assessment (DPIA) in any major project involving the use of personal data.

17.2. The College will consider whether to do a DPIA if we plan to carry out any other:

- evaluation or scoring;
- automated decision-making with significant effects;
- systematic monitoring;
- processing of sensitive data or data of a highly personal nature;
- processing on a large scale;
- processing of data concerning vulnerable data subjects;
- innovative technological or organisational solutions;
- processing that involves preventing data subjects from exercising a right or using a service or contract.

17.3. We always carry out a DPIA if we plan to:

- use systematic and extensive profiling or automated decision-making to make significant decisions about people;
- process special-category data or criminal-offence data on a large scale;
- systematically monitor a publicly accessible place on a large scale;
- use innovative technology in combination with any of the criteria in the European guidelines;
- use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit;
- carry out profiling on a large scale;
- process biometric or genetic data in combination with any of the criteria in the European guidelines;
- combine, compare or match data from multiple sources;
- process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines;
- process personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;
- process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;
- process personal data that could result in a risk of physical harm in the event of a security breach.

17.4. We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.

17.5. If we decide not to carry out a DPIA, we document our reasons.

18. STAFF RESPONSIBILITIES

All staff are responsible for working in compliance with Data Protection Legislation and the conditions of the College Data Protection Policy.

Staff must ensure they:

i. Adhere to all Data Protection and IT related policies and procedures, particularly this policy, and the Personal Portable Devices Policy.

ii. Address any questions or concerns about Data Protection to the Data Protection Officer. Any breach of the Data Protection Policy may lead to disciplinary action being taken**.**

iii. Undertake Mandatory Data Protection training.

19. DATA SUBJECT RESPONSIBILITIES

All data subjects are responsible for:

i. Ensuring that any personal information they provide in connection with their employment, registration or other contractual agreement is accurate.

ii. Informing the College of any changes to personal information that they have provided: address, bank details, etc.

iii. Responding to requests to check the accuracy of the personal information held on them and processed by the College, and informing the College of any errors or changes to be made.

20. DATA SUBJECT RIGHTS

20.1. Data subjects have a number of rights. They can:

- access and obtain a copy of the information the College holds about them, on request;
- require the College to change incorrect or incomplete data;
- require the College to delete or stop processing their data, for example where the data is no longer necessary for the purposes of processing;
- object to the processing of their data where the College is relying on its legitimate interests as the legal ground for processing.

20.2. They may exercise any of these rights, or otherwise complain about the way the College is processing their data, by contacting the Data Protection Officer at info@llnations.ac.uk .

20.3. They also have the right to complain to the data protection supervisory authority, The UK Information Commissioner's Office (ICO) who can be contacted at https://ico.org.uk/concerns/handling.

21. ROLES, RESPONSIBILITIES, POLICY APPROVAL AND REVIEW

21.1. The **Board of Trustees** have legal oversight and responsibility for all College policies, providing leadership and active support for them and are responsible for:

- Ensuring a legally compliant and fit for purpose data protection policy is in place and approved by them.
- Ensuring satisfactory arrangements are made for its effective implementation, including the provision of resources.
- Ensuring the Senior Leadership Team monitors, evaluates and periodically reviews this policy and recommends any changes to first the Governance Committee and then the Board of Trustees for approval.
- Ensuring complaints and appeals brought under the terms of this policy are managed satisfactorily by the Senior Leadership Team.
- Ensuring decision making complies with all relevant legislation and regulatory bodies.
- Ensuring they receive details from the Senior Leadership Team of reported incidents of data breaches and outcomes of cases (particularly where a significant impact on someone has occurred or lessons need to be learned), or of a serious incident or one which could be of reputational risk to the College which should be reported to either the Information Commissioner's Office, the Office for Students and/or the Charity Commission.

21.2. The **Principal/CEO and Senior Leadership Team** are responsible for:

- The implementation and management of this policy; ensuring that procedures are implemented consistently and with clear lines of authority and actively and visibly leading the College's data protection policy and practice.
- Ensuring this policy is continually improved in consultation with students and staff.
- Monitoring, evaluating and periodically reviewing this policy and for obtaining approval from the Board of Trustees for any changes made.

- The management of complaints.
- Ensuring decision making complies with all relevant regulatory bodies.
- Reporting details to the Board of Trustees of reported incidents of data breaches, outcomes of cases (particularly where significant impact on someone has occurred or lessons need to be learned), or of a serious incident or of one which could be of reputational risk to the College.

21.3. The **Principal/CEO, Senior Leadership Team, and all department heads, staff and students** have a responsibility for ensuring that the principles of this policy are incorporated into all aspects of project planning, IT planning and management and data management, retention and storage.

21.4. Through their ongoing regular meetings, the **Head Students and the Principal/CEO** have a responsibility to provide an opportunity for matters related to this policy to be raised with all members of the student body (the Head Students), the Senior Leadership Team and the Board of Trustees (the Principal/CEO).

21.5. **Any person covered by the scope of this policy** is responsible for:

- familiarising themselves with this policy on appointment/at induction/orientation or when their personal data is processed or stored by the College;
- demonstrating active commitment to this policy by:
  - processing, storing or retaining data as per this policy;
  - supporting anyone who either makes a data request or complains about the handling of their data including supporting them to make a formal complaint if appropriate;
- , if involved in a compliant in any capacity:
  - ensuring they present their case with integrity and in a timely fashion and/or
  - ensuring they comply with any investigation and the procedures in this policy.

21.6. The College entrusts **all individuals across the institution** to take a pro-active role in improving the College's data protection policy and practice.

21.7. The **Head of Operations** is responsible for dealing with all data breaches, complaints and data subject access requests on behalf of the Senior Leadership Team.

21.8. **Staff** responsibilities can be found in section 18 of this policy above.

21.9. **Data Subject** responsibilities can be found in section 19 of this policy above.

21.10. Whilst the College is the data controller, **all data users** are individually responsible for complying with the law and this policy. Failure to comply with this policy and/or with data protection legislation may result in disciplinary action by the College.

22. POLICY AND PRIVACY NOTICE COMMUNICATION

22.1. To fulfil the transparency requirements of the DPA, data subjects have a right to be given certain information at the time when their personal data is obtained, or soon after if the personal data is not obtained directly from data subjects. This information is provided in the form of a privacy notice.

22.2. Information provided to data subjects must be in clear and plain language, and must be concise, transparent, intelligible and easily accessible.

22.3. A privacy notice must contain the following information about a data subject's personal data:

i. What data is collected
ii. How the data is collected including whether it is accessed from third parties
iii. Why the data is processed
iv. The legal basis for processing the data

v. Who has access to the data
vi. Which, if any, third parties will have access to the data and why
vii. Specific information about any sensitive or special category data processing
viii. How the data is protected
ix. For how long it is retained
x. The consequences of not providing the data.
xi. The rights of the data subject, including their right to access, amend, delete, object to the processing of the data or complain about how it is processed

Information that is already in the public domain is exempt from the DPA.

22.4. This policy together with all other College policies mentioned in this document can be found on the College website: www.allnations.ac.uk and in the full in the student area on the College VLE.

22.5. Privacy Notices are stored in the 'Privacy at All Nations' page of the College website: www.allnations.ac.uk

22.6. When personal data is collected other than via the website, a telephone caller or email enquirer must be given the relevant privacy notice information at the point of data collection, by the member of staff dealing with their enquiry.

22.7. The College Administrator will make every effort to respond to any request to provide this policy in a different format. Such requests should be sent to info@allnations.ac.uk

22.8. This policy will be included in staff and student induction and all other groups whose data we process must be made aware of the policy and relevant privacy notice when their data is collected.

23. APPENDICES

1. DPA Monitoring Form
2. Data Protection Impact Assessment

Appendix 1

ALL NATIONS CHRISTIAN COLLEGE

DPA MONITORING FORM

Number of complaints received or concerns raised at College since last meeting	
If a complaint/concern has been lodged: Nature of Complaint/Concern: (informal or formal; whether ICO was informed):	Date complaint logged:
Description of Complaint/Concern(s):	
College response:	
Action to be considered to mitigate future risk?	
Any staff training to be implemented?	

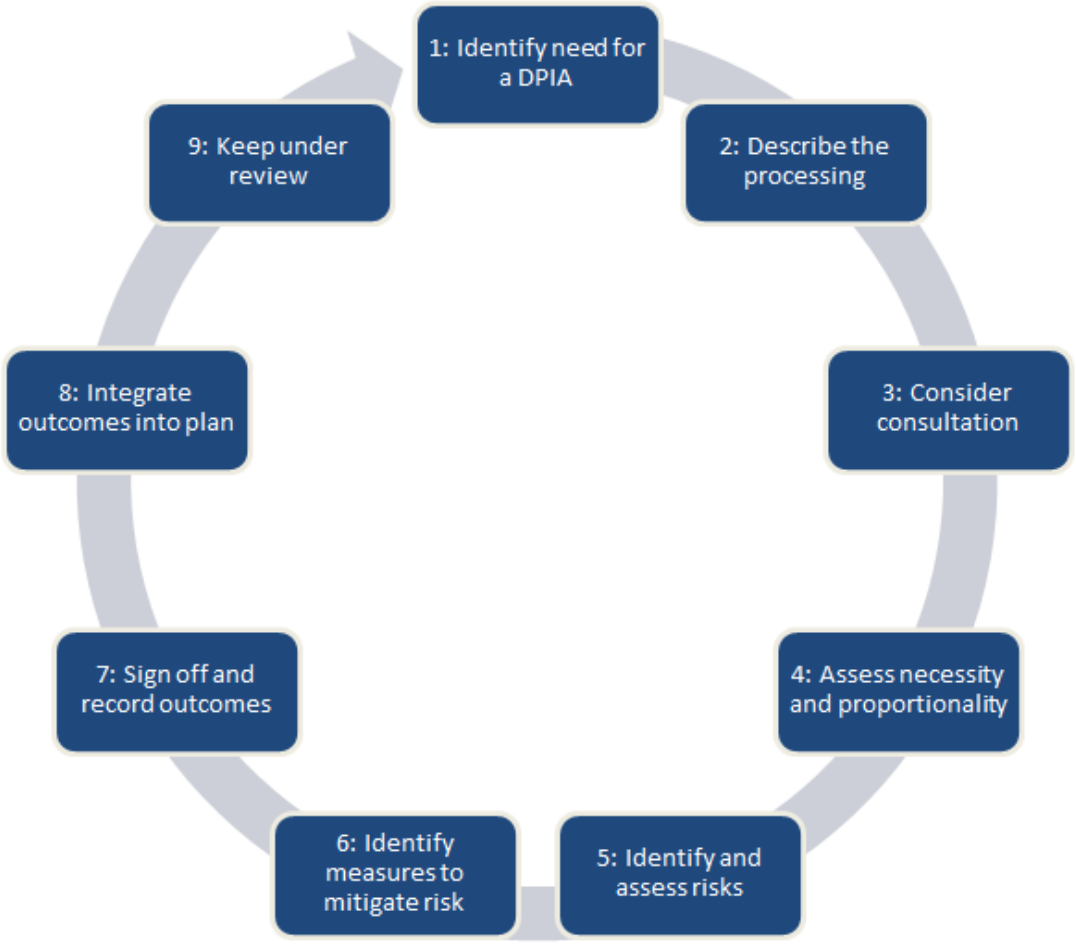
Appendix 2

ALL NATIONS CHRISTIAN COLLEGE
DATA PROTECTION IMPACT ASSESSMENT

WHEN TO CARRY OUT A DPIA

The College will consider carrying out a Data Protection Impact Assessment (DPIA) when planning a major project involving the use of personal data. The assessment should be done before any new procedures that involve processing personal data and run alongside the planning and development process. Please see section 17 of the All Nations Data Protection Policy.

Below is a diagram to show the steps the DPIA process should follow:



Please fill out the following form if you are at the start of planning a major project involving the use of personal data, or if you are making a significant change to an existing process. NB The final outcomes should be integrated back into your project plan.

ALL NATIONS CHRISTIAN COLLEGE
DATA PROTECTION IMPACT ASSESSMENT FORM[1]

Submitting controller details

Name of controller	
Subject / title of Data Protection Officer *(DPO)*	
Name of controller contact / DPO *(delete as appropriate)*	

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves: *You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.*

[1] https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf

Step 2: Describe the processing

Describe the nature of the processing:
How will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing:
What is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing:
What is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing:
What do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: *Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?*

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: *What is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?*

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. *Include associated compliance and corporate risks as necessary.*	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA