allnations
training for mission

APPROPRIATE POLICY DOCUMENT

Document Title		
APPROPRIATE POLICY DOCUMENT		
Document Author/Owner:	**Responsible Person:**	
Matt Soleye	Chief Executive Officer, SLT	
Approving Body:	**Date of Approval:**	
Board of Trustees		
Effective from:	**Review Date:**	**Edition:**
31.03.2026	31.03.2027	1
EITHER For Public Access? **Tick as appropriate**	**OR** For Internal Access only? **Tick as appropriate**	
YES ✓	**YES**	

Summary/Description:

An Appropriate Policy Document (APD) is required under the Data Protection Act 2018 when processing special category and criminal offence data under certain conditions. It explains how the organisation complies with the UK General Data Protection Regulation, particularly in relation to lawful processing and retention and supports the Record of Processing Activities. The APD must be kept under review, retained for six months after processing ends and provided to the Information Commissioner's Office if requested.

2025-26 v1
Sep 25
First iteration published of this policy

ALL NATIONS CHRISTIAN COLLEGE

To cultivate biblically rooted, hope-filled and culturally relevant engagement with God's mission, by training and equipping disciples of Jesus Christ in partnership with the global church.

APPROPRIATE POLICY DOCUMENT POLICY

1 CONTENTS OF POLICY

Table of Contents

2 INTRODUCTION

2.1 The Data Protection Act 2018 requires the College to maintain an Appropriate Policy Document (APD) where it processes special category and criminal offence data under certain specified conditions. In particular, this applies to processing carried out under the substantial public interest conditions set out in Schedule 1, as well as processing relating to employment, social security and social protection.

2.2 This document sets out how All Nations Christian College ensures that the processing of such data complies with the principles of the UK General Data Protection Regulation, including lawful, fair and transparent processing and appropriate retention and disposal. It should be read alongside the College's wider data protection framework and supports its Record of Processing Activities under Article 30.

2.3 The College processes special category personal data as part of its educational, pastoral and safeguarding functions. This may include information relating to religious beliefs, health, equality and diversity and safeguarding matters. Criminal offence data may also be processed where necessary for safeguarding, recruitment or to meet legal obligations.

2.4 This processing relates primarily to students, applicants, staff, volunteers, missionaries-in-residence and other individuals engaging with the College in its capacity as a Christian higher education provider. The College ensures that appropriate safeguards are in place to protect this data and that individuals are provided with clear information about how their data is used and retained.

3 LEGISLATIVE FRAMEWORK

3.1 Legislative Obligations:

The College has a duty to comply with the following data protection and information governance legislation:

- The UK General Data Protection Regulation ("UK GDPR"), in particular Article 25, which requires the implementation of data protection by design and by default.
- The Data Protection Act 2018, which supplements the UK GDPR and sets out the UK's data protection framework.
- The Privacy and Electronic Communications Regulations (PECR) 2003 (as amended), which govern electronic communications, including marketing and the use of cookies.
- The Human Rights Act 1998, in particular Article 8 of the European Convention on Human Rights, which provides for the right to respect for private and family life.

- The Freedom of Information Act 2000, which provides rights of access to information held by public authorities and must be balanced with data protection obligations.

Processing of special category and criminal offence data is carried out in accordance with the relevant conditions set out in Schedule 1 of the Data Protection Act 2018 and supported by a lawful basis under Article 6 of the UK GDPR, as recorded in the College's Record of Processing Activities.

3.2 Duty of Care:

The College must also meet its general duty of care obligations to students, staff, volunteers, Missionaries in Residence and visitors by ensuring that personal data is handled securely, responsibly and in a way that protects individuals from harm, including risks associated with unauthorised access, misuse or loss of personal data.

3.3 Related Documents:

The College has developed policies and procedures to support compliance with its data protection obligations. These documents are available on request and should be read in conjunction with this policy:

- Data Protection Policy
- Information Governance Framework
- ICT General Policy / Acceptable Use of ICT Policy
- Data Retention Schedule
- Data Breach Response Procedure
- Records of Processing Activities (ROPA)
- Safeguarding Policy

4 DESCRIPTION OF DATA PROCESSED

4.1 All Nations Christian College processes Special Category personal data (SC data) as part of its educational, pastoral and safeguarding responsibilities. This may include:

- Religious beliefs (e.g. spiritual formation, participation in Christian activities)
- Health data (e.g. medical conditions, disabilities, counselling support needs)
- Equality and diversity data (e.g. ethnicity, nationality where relevant)
- Safeguarding-related information where applicable

4.2 Criminal Offence data (CO data) may be processed where necessary for safeguarding, recruitment or legal obligations.

4.3 This processing relates primarily to students, applicants, staff, volunteers, missionaries-in-residence (MIR) and other individuals engaging with the College, in line with its role as a Christian higher education provider.

5 SCHEDULE 1 CONDITION FOR PROCESSING

5.1 The College relies on the following Schedule 1 conditions under the Data Protection Act 2018:

- Paragraph 1 – Employment, social security and social protection
- Paragraph 6 – Statutory and government purposes
- Paragraph 8 – Equality of opportunity or treatment
- Paragraph 10 – Preventing or detecting unlawful acts (where applicable)
- Paragraph 18 – Safeguarding of children and individuals at risk
- Paragraph 12 – Religious bodies (where processing relates to religious beliefs within the College community)

5.2 Processing is also supported by a lawful basis under Article 6 of the UK GDPR (e.g. consent, contract, legal obligation or legitimate interests), as outlined in the College's Data Protection Policy.

6 PROCEDURES FOR ENSURING COMPLIANCE WITH THE PRINCIPLES

6.1 Accountability principle: The College maintains appropriate documentation of its processing activities, including records under Article 30. Data protection policies, including the Data Protection Policy, are reviewed regularly and approved by the Board of Trustees. Data Protection Impact Assessments (DPIAs) are undertaken where processing is likely to result in high risk to individuals, particularly where sensitive or special category data is involved.

6.1.1 Principle (a): lawfulness, fairness and transparency

The College ensures that all processing has a clear lawful basis under Article 6 of the UK GDPR and, where required, a Schedule 1 condition. Individuals are provided with clear privacy information explaining how their data is used, including through privacy notices and student communications. Processing is carried out fairly and individuals are not misled about how their data will be used.

6.1.2 Principle (b): purpose limitation

Personal data, including special category data, is collected for specific, explicit and legitimate purposes such as education, pastoral care, safeguarding and compliance with legal obligations. The College does not use personal data for incompatible purposes unless required by law or with appropriate consent.

6.1.3 Principle (c): data minimisation

The College ensures that only data which is necessary and relevant for its stated purposes is collected and processed. Data is limited to what is required to support students, fulfil contractual and legal obligations and maintain appropriate safeguarding and welfare standards. Regular reviews are undertaken to ensure data remains relevant.

6.1.4 Principle (d): accuracy

The College takes reasonable steps to ensure personal data is accurate and kept up to date. Processes are in place to allow individuals to request corrections and inaccuracies are rectified without delay. Records are reviewed periodically to maintain accuracy.

6.1.5 Principle (e): storage limitation

Personal data is retained only for as long as necessary to fulfil its purpose, in line with the College's Data Retention Schedule. Data is securely deleted or anonymised when no longer required, unless retention is required by law.

6.1.6 Principle (f): integrity and confidentiality (security)

The College implements appropriate technical and organisational measures to protect personal data, including:

- Access controls on a need-to-know basis
- Secure storage of physical and electronic records
- Password protection and encryption where appropriate
- Staff confidentiality obligations
- Secure disposal of data

These measures are proportionate to the sensitivity of the data being processed.

7 RETENTION AND ERASURE POLICIES

7.1 The College retains special category and criminal offence data only for as long as necessary to fulfil the purposes for which it was collected, including:

- Student records: retained in line with academic and regulatory requirements
- Safeguarding records: retained in accordance with safeguarding guidelines
- Health and support data: retained for the duration of support needs and for a limited period thereafter

7.2 All data is securely deleted, anonymised or destroyed in accordance with the College's Data Retention Schedule once no longer required. Data is not retained longer than necessary unless required by law or regulatory obligations.

8 ROLES, RESPONSIBILITIS, POLICY APPROVAL AND REVIEW

8.1 The Board of Trustees has overall accountability for ensuring that the College complies with its legal obligations under the Data Protection Act 2018 and the UK General Data Protection Regulation. The Board is responsible for ensuring that appropriate policies, resources, and governance arrangements are in place to support the lawful processing of personal data, including special category and criminal offence data.

8.2 The Chief Executive Officer (CEO) and Senior Leadership Team (SLT) are responsible for ensuring that this Appropriate Policy Document is effectively implemented across the College and that appropriate organisational and technical

measures are maintained to protect personal data. They are also responsible for ensuring that data protection risks are appropriately managed and escalated where necessary.

8.3 The designated Responsible Person (Data Protection Lead) is responsible for overseeing compliance with this policy, including:

- Ensuring that processing of special category and criminal offence data aligns with the conditions set out in Schedule 1 of the Data Protection Act 2018
- Maintaining and reviewing the Record of Processing Activities (ROPA) under Article 30 UK GDPR
- Advising on Data Protection Impact Assessments (DPIAs) where required
- Monitoring compliance with data protection principles and reporting any risks or incidents

8.4 Heads of Department and Managers are responsible for ensuring that personal data within their areas is processed in accordance with this policy, relevant legislation, and College procedures. This includes ensuring that staff understand their responsibilities and that appropriate safeguards are in place for handling sensitive data.

8.5 All staff, volunteers, and individuals acting on behalf of the College are responsible for:

- Familiarising themselves with this policy and related data protection policies
- Ensuring that personal data is handled securely and in accordance with College procedures
- Reporting any data protection concerns, risks, or incidents promptly in line with the Data Breach Response Procedure

8.6 This Appropriate Policy Document will be reviewed annually, or sooner where there are changes to legislation, regulatory requirements, or the College's processing activities. The policy will remain in place and be retained for six months after the College ceases processing the relevant special category or criminal offence data, in accordance with Schedule 1 of the Data Protection Act 2018.

9 RELATED POLICY DOCUMENTS

Legislation

- UK Data Protection Act 2018
- UK Data Usage and Access Act 2025
- UK General Data Protection Regulation 2018

Policy

- All Nations Christian College Academic Use of Generative AI Policy
- All Nations Christian College Acceptable Use of ICT Policy
- All Nations Christian College Data Protection Policy
- All Nations Christian College Email Communications Services Policy
- All Nations Christian College ICT General Policy and Procedures
- All Nations Christian College Social Media Policy

Guidance - Glossary | ICO;

If you would like this document in a different format (e.g. large print, braille), please contact cta@allnations.ac.uk.

If you need any assistance to access or understand the document, please contact cta@allnations.ac.uk.

All printed versions of this document are classified as uncontrolled. Please ensure you access the current version from the Policy Website Page.