allnations
training for mission

INFORMATION AND COMMUNICATIONS TECHNOLOGY GENERAL POLICY AND PROCEDURES 2021-22

Document Title		
INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) GENERAL POLICY AND PROCEDURES		
Document Author and Department:	**Responsible Person and Department:**	
Information and Learning Services Manager (ILSM) Information and Learning Services	Head of Operations and ICT Manager	
Approving Body:	**Date of Approval:**	
Senior Leadership Team	16th February 2022	
Date coming into force:	**Review Date:**	**Edition No:**
16th February 2022	Annually	3
EITHER For Public Access? **Tick as appropriate**	**OR** For Internal Access only? **Tick as appropriate**	
YES ✓	**YES**	

Summary/Description:

This document sets out all the details pertaining to the use of Information and Communications Technology at All Nations Christian College including those validated by The Open University.

This document has been adapted from policy documents by INF International, with grateful acknowledgment.

Reviewed August 2021 – *amended staff and team title changes*

Reviewed February 2022 - amended *Roles, Responsibilities, Policy Approval and Review section* to bring them into line with other policies.

ALL NATIONS CHRISTIAN COLLEGE

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

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) GENERAL POLICY AND PROCEDURES

1 CONTENTS OF POLICY

2 INTRODUCTION

Information and Communications Technology (ICT) is integral to the effective operation of All Nations Christian College. The purpose of this policy is to ensure good practice in the provision and use of ICT facilities administered by All Nations Christian College and relates to the provision of services. It applies to all students, staff (permanent and temporary), volunteers, voluntary workers, guests, external library users and conference delegates. This policy applies to all ICT equipment owned or leased by All Nations and to personal equipment and devices connected any network, or system, owned or leased by All Nations.

3 LIST OF ICT RELATED DOCUMENTS

In addition to the contents of this policy, users must abide by other policies or codes as relevant, including:

- Information and Communications Technology (ICT) General Policy and Procedures
- Social Media Policy
- Portable Devices Policy
- Email Communication Services Policy
- Data Security Analysis
- ICT Disaster Recovery Plan
- External IT Support
- IT Staffing Structure

4 LEGISLATIVE FRAMEWORK

This policy contains rules and regulations of the College which have been prepared in line with Open University regulations and, where appropriate, the requirement of the Office for Students' Regulatory Framework and the UK Quality Code for Higher Education. This policy also

complies with the Equality Act 2010, the Data Protection Act 2018 and the Counter-Terrorism and Security Act 2015.

5 DEFINITIONS

Accessibility	The extent to which a service can be used by people with disabilities or special access requirements.
Firewall	A piece of computer hardware or software application that stops unauthorised communication from an external network (such as the internet) reaching a client computer.
Filtering	A piece of software that processes data before passing it to another application, for example to reformat characters or to remove unwanted types of material (Oxford English Dictionary).
Hardware	The physical components of a computer or computer system, including peripheral devices such as monitors and printers (Oxford English Dictionary).
ICT	Information and Communications Technology.
Portable Devices	Mobile phones, tablets, laptops, notebooks.
Software	The programs and other operating information used by a computer (Oxford English Dictionary).
User	Students, staff (permanent and temporary), volunteers, voluntary workers, guests, external library users and conference delegates.
VLE	Virtual Learning Environment – a set of learning and teaching tools based on networked computer resources that provide a focus for students' learning activities and their management and facilitation, along with the provision of content and resources required to help make the activities successful.
Wi-Fi	a facility allowing computers, smartphones, or other devices to connect to the Internet or communicate with one another wirelessly within a particular area (Oxford English Dictionary).

Unless specified, ICT definitions are taken from JISC, E-Assessment Glossary (Extended), 2006.

6 COLLEGE COMMITMENT

6.1 PROVISION

6.1.1 All Nations is committed to provide ICT facilities (appropriate hardware and software) that enable students to access the materials that they need to be able to pursue their studies. This includes the provision of internet facilities in order to access learning and information resources. Examples of such provision include:

- The provision of internet facilities in order to access learning and information resources, and support to be able to use those facilities.
- Ensuring that lecture rooms have appropriate audio and visual display equipment to deliver lectures and student presentations.

6.1.2 All Nations is committed to provide appropriate ICT facilities (appropriate hardware and software) to enable each member of staff or volunteer to carry out their work effectively and

communicate with others. It recognises that the nature of this provision may vary depending on the nature of the work that is to be fulfilled. Such provision includes:

- The supply of desktop and laptop computers, and if needed portable devices
- The provision of appropriate software for particular tasks (e.g. accounting, word processing software)
- The provision of sufficient space to be able to store electronic documents and email communications

6.1.3 All Nations is committed to provide sufficient internet and Wi-Fi services for external library users and conference delegates to be able to use portable devices and (in the case of delegates attending All Nations' short courses) to access necessary learning and information resources.

6.1.4 All Nations is committed to providing ICT facilities impartially. The College makes every effort, in accordance with its **'Equality and Diversity Policy'** to ensure that students are not unlawfully discriminated against because of the Equality Act 2010 'protected characteristics of age, disability, gender reassignment, pregnancy and maternity, marriage and civil partnership, race (including colour, ethnic/national origin or nationality), religion or belief, sex (gender) and sexual orientation. The College believes that diversity is a positive contribution to the learning experience at All Nations.

6.2 SUPPORT

All Nations is committed to providing timely support to students, staff, volunteers and voluntary workers in the use of the College's ICT facilities. This support may be in partnership with, or involve third parties. Such support includes:

- Staff and volunteer training on the use of appropriate hardware and software
- Technical support in the event of the failure of computer and communication systems and services.
- Assistance to students in the use of ICT facilities (in conjunction with student support systems).

6.3 ACCESSIBILITY

All Nations recognises its ethical and legal responsibility (e.g. under the Equality Act 2010) to provide ICT facilities that are accessible to all, including those with disabilities, health conditions and learning difficulties. Such provision includes:

- Ensuring that the College website and virtual learning environments (VLEs) comply with accessibility regulations and guidelines
- The provision of accessible hardware and software for staff, volunteers, voluntary workers and students who require it.
- Assistance securing additional accessible equipment for students eligible for external support (See also Learning Support Policy)

6.4 PROTECTION

6.4.1 All Nations recognises its ethical and legal responsibility to protect its users from harm, including but not limited to:

- malware, unsolicited mail loss of privacy, identity theft, pornography, violence, extremism, incitement, all forms of bullying and harassment, victimisation (See also **Acceptable Use of Information and Communications Technology (ICT) Policy**),

6.4.2 Measures to prevent this from happening include:

- Ensuring awareness of the College's various ICT policies, especially the **Acceptable Use of Information and Communications Technology (ICT) Policy**
- Providing both information and training on appropriate and effective use of ICT facilities

- Promoting an atmosphere conducive to raising concerns where policies and procedures are not being followed
- Technical solutions including but not limited to firewalls and filtering software.

7 USER RESPONSIBILITIES:

The responsibility of users is to:

- Use the resources provided to them within the framework of this and other related College ICT policies, particularly the **Acceptable Use of Information and Communications Technology (ICT) Policy**
- Notify the College's Information and Learning Services Manager (ILSM) of anything that prevents them working within the framework of this and other related policies
- Notify the ILSTM if they become aware of a third party breaching the College policy on Acceptable Use of ICT Facilities.
- Abide by the terms of the College's Code of Conduct (see **Conduct, Conflict and Student Disciplinary Policy**)

8 COMPLAINTS AND APPEALS

Should a user wish to raise a concern about the ICT provision (with the exception of 9.5 below), they should initially discuss this with the College's ICT Manager who will seek to address their issues in conjunction with other members of the ICT Team or the Head of Operations. If they are still unhappy with the level of service provided or appeal against a decision reached they do so using the College **Complaints Policy and Procedure.**

9 DISCIPLINARY PROCEDURES

9.1 The College hopes that all users will enjoy studying/working at All Nations and will observe the rules and standards for ICT use and general behaviour that which have been set in the **Acceptable Use of ICT Facilities Policy,** and the **College Code of Conduct**. However, in the event of a failure to do so, then disciplinary measures will be taken and in certain circumstances other statutory bodies informed.

9.2 Serious infringements may necessitate taking legal advice or involve the police (for example in cases which involve a criminal offence or activities which could put others at risk). In the case of:

- Accusations of misconduct by **students**, these will be investigated in accordance with the College **Conduct, Conflict and Student Disciplinary Policy and Procedures;**

- accusations of misconduct by members of **staff, including voluntary workers,** these will be investigated using the **College Staff Disciplinary Policy and Procedure** document, which is available from the College Administrator;

- accusations of misconduct by **volunteers,** these will be investigated by the College Administrator in discussion with the Senior Leadership Team

- accusations of misconduct by **External Library Users**, these will be investigated by the Information and Learning Services Manager in discussion with the Librarian, and Senior Leadership Team.

- accusations of misconduct by **Conference Delegates,** these will be investigated by the Conference Manager in discussion with the Senior Leadership Team.

10 ROLES, RESPONSIBILITIES, POLICY APPROVAL AND REVIEW

10.1 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 that:

- A legally compliant and fit for purpose ICT policy is in place and approved by the Senior Leadership Team.
- Satisfactory arrangements are made for its effective implementation, including the provision of resources.
- They receive details from the Senior Leadership Team of any serious incident or one which could be of reputational risk to the College which should be reported to either the Office for Students and/or the Charity Commission.

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

- The implementation, management and approval of this policy; ensuring that procedures are implemented consistently and with clear lines of authority and actively and visibly leading the College's ICT policy and practice.
- Ensuring this policy is continually improved in consultation with students, staff and the ICT department.
- Ensuring any formal complaints are managed appropriately by the Head of Operations and the ICT department and in line with the College complaints policy.
- The management of the appeals process.
- Ensuring decision making complies with all relevant regulatory bodies.
- Ensuring they receive details from the Head of Operations and ICT Manager of reported incidents 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.
- Reporting details to the Board of Trustees of any serious incident or one which could be of reputational risk to the College.

10.3 The Head of Operations is responsible for:

- Ensuring this policy is monitored evaluated and periodically reviewed by the ICT Manager, in consultation with the Head of Operations, and any changes are recommended to the Senior Leadership Team for their approval.
- Managing formal complaints brought under the terms of this policy in line with the College Complaints policy.
- Ensuring decision making complies with all relevant legislation and regulatory bodies.
- Reporting to the Senior Leadership Team incidents 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.

10.4 The ICT Manager is responsible for:

- The day to day management of ICT provision in the College.
- , in consultation with staff and students, monitoring, evaluating and periodically reviewing this policy in consultation with the Head of Operations.
- The management of informal complaints.

10.5 The **Principal/CEO, Senior Leadership Team, and all department heads,** are responsible for ensuring that the principles of this policy are implemented through:

- incorporating them into the strategic direction of the College;
- constantly seeking to improve the information and service provided;
- exploring what can be learned from complaints when they occur.

10.6 Through their ongoing regular meetings, the **Head Students** and the **Principal/CEO** are responsible for using this meeting to raise and resolve issues of mutual concern with the student body and/or The Senior Leadership Team/Board of Trustees as relevant.

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

- familiarising themselves with this policy on appointment/at induction/orientation;
- taking a proactive role in improving this policy ;
- demonstrating active commitment to this policy by:
  - using the College network facilities responsibly, safely and with due consideration for others;
  - notifying the ICT department when ICT equipment is faulty;
  - supporting anyone who makes a formal complaint if appropriate;
- , if **involved in a complaint** 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.

10.8 **College and Recruitment and Training Administrators** are responsible for managing the administration of the complaints and appeals processes.

11 POLICY COMMUNICATION

11.1 This policy and any other policies referred to in this document can be found on the College website: www.allnations.ac.uk and in the student area on the College VLE.

11.2 The **Staff Disciplinary Procedure** can be found in the Staff Handbook Appendices which is obtainable from the College Administrator at info@allnations.ac.uk

11.3 The Student Disciplinary Procedure can be found in the College **Conduct, Conflict and Student Disciplinary Policy and Procedures**.

11.4 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

11.5 This policy will be included in staff and student induction and available to External Users of the College ICT system.

12 RELATED DOCUMENTS

In addition to the ICT related policies in section 2, the following College documents are related to this policy:

- All Nations Christian College Undergraduate Handbook
- All Nations Christian College Postgraduate Handbook
- All Nations Christian College Student Handbook
- All Nations Christian College Learning Support Policy
- All Nations Christian College Equality and Diversity Policy
- All Nations Christian College Data Protection Policy
- All Nations Christian College Harassment Policy
- All Nations Christian College Complaints Policy

13 APPENDIX

- Guidance on Use of IT Facilities

GUIDANCE ON USE OF IT FACILITIES

a. You may use College IT facilities for purposes related to college work or study, and for a limited and reasonable amount of personal use. Such use is a privilege and not a right and must not inhibit or interfere with the use by others for College purposes.

b. Staff, and students must not use College IT facilities for outside work, whether paid or unpaid, or for non-College activities which generate income, except by explicit permission of the Principal/CEO or as part of an agreed role.

c. You must not use College IT facilities to engage in any unlawful activity, or to infringe College Regulations.

d. You must not use College IT facilities without permission. This includes using computers and networks, or accessing, copying, reading, or storing software, databases, messages or data. You must not attempt to gain unauthorised access to any College IT facilities, or use College facilities to gain unauthorised access to other IT facilities.

e. You must not deliberately or recklessly act in a way which directly or indirectly causes disruption to others' use of College IT facilities, or so use College IT facilities to disrupt the use of IT facilities elsewhere.

f. In general, systems and application software that is installed or otherwise available within the College is protected by license agreements. You must not use such software unless you have permission to use it under College license agreements. You must not copy software which is installed or otherwise available unless you have explicit permission or own a license which permits you to do that.

g. You must not knowingly download, transmit, store, generate or use any programme, tool or virus designed to damage or disrupt or in any other way interfere with the functioning of IT facilities. You must take sufficient care to minimise the risk of doing this inadvertently. If you suspect you have a virus then you must take action to eliminate it.

h. You must treat as confidential any information to which you gain access in using College IT facilities and which is not on the face of it intended for unrestricted dissemination. You must not copy, modify or disseminate such information without explicit permission from an authorised person. The ability to read or alter information held on a computer system does not imply permission to do so.

i. Any information about living individuals must be held in accordance with College policy and the responsibilities as a Data User under the Data Protection Act 1998.

j. In order to ensure effective running of IT services, or to manage costs, the College from time to time imposes controls on the use of systems. An example is the use of firewalls in some areas of the College. You must not attempt to circumvent such controls.

k. You must not use College IT facilities to create, transmit, store, download or display any illegal, offensive, obscene, indecent or menacing images, data or other material, or any data capable of being resolved into such material.

l. You must not use College IT facilities to defame, harass, offend or hinder another person, by creation, transmission, storage, download or display of materials, or by other means.

m. You must not send an email or message that does not correctly identify you as the sender, or which appears to originate from another person, or otherwise attempt to impersonate another person. You must not send unsolicited emails to a large number of recipients, without proper authorisation to do so, or unless the recipients have indicated an interest in or consented to receiving such email.

n. You must not use College IT facilities to create, access, store or transmit material in a way which infringes a copyright, trade mark, or other intellectual property right.

o. You must not cause damage to College-owned IT facilities, or move or remove such facilities without authorisation. Any damaged or faulty facilities should be reported so that repairs can be made.

p. You must use a secure paying mechanism if using College cards online. Look for a padlock at the top or bottom of the web page. A bank or website will never ask for confirmation of login details or account information in an e-mail or any other message.