allnations
training for mission

ACCEPTABLE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) POLICY AND PROCEDURES 2021-22

Document Title		
ACCEPTABLE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) POLICY AND PROCEDURES		
Document Author and Department:	**Responsible Person and Department:**	
Head of 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	2
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 Acceptable Use of Information and Communications Technology (ICT) at All Nations Christian College including those validated by The Open University.		
This document has been adapted from INF International's ICT Appropriate Usage Policy, with grateful acknowledgment.		
Reviewed August 2021 (made minor grammatical changes, amended job titles) Reviewed 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.

ACCEPTABLE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) POLICY AND PROCEDURES

1 CONTENTS OF POLICY

2 INTRODUCTION

Information and Communication Technologies (ICT) have become an integral, necessary, and strategic part of the operations of All Nations Christian College (the College). Observing the College's values while using ICT systems should ensure that all users remain safe and that ICT systems are always available for normal College operations. The purpose of this policy is to define acceptable, and unacceptable, usage of the College's ICT systems in line with the College's established values and culture of openness, trust and integrity (see Section 7).

3 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. It also complies with Counter Terrorism and Security Act 2015 and the Data Protection Act.

4 SCOPE

4.1 College is committed to protecting its employees, volunteers, voluntary workers, partners, clients and itself from damaging or illegal actions by individuals, either knowingly or unknowingly. Inappropriate use exposes the College, and individuals, to risks including virus attacks, compromise of network systems and services, legal issues, threats to personal security and damaging the reputation of the organisation.

4.2 This policy applies to all ICT equipment owned or leased by the College and to personal equipment and devices connected any network, or system, owned or leased by the College (including but not limited to computer equipment, telephone, fax , software, operating systems, storage media, data files, network accounts, electronic mail, and web-browsing). These systems are for the purpose of serving the interests of College users in the course of normal operations.

4.3 All users of the College network facilities are required to agree in writing to abide by this policy before permission is given to access the College's ICT facilities, regardless of whether they are using College or personal devices.

5 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

6 DEFINITIONS*

Accessibility:	The extent to which a service can be used by people with disabilities or special access requirements.
Blogging:	Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.
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 (OED).
Hardware:	The physical components of a computer or computer system, including peripheral devices such as monitors and printers (OED).
ICT:	Information and Communications Technology.
Portable Devices:	Mobile phones, tablets, laptops, notebooks.
Software:	The programs and other operating information used by a computer (OED).
Spam:	Unauthorised and/or unsolicited electronic mass mailings (INF).
Social Media:	Websites and applications that enable users to create and share content or to participate in social networking.
Social Networking:	The use of dedicated websites and applications to interact with others or to find people with similar interests to one's own.
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 (OED).

* ICT definitions are taken from JISC, E-Assessment Glossary (Extended), 2006, unless marked OED (Oxford English Dictionary).

7 COLLEGE GENERAL CODE OF CONDUCT

7.1 This policy is embedded within the terms of the College's Code of Conduct. (See the College **Conduct, Conflict and Student Disciplinary Policy and Procedure**).

7.1 The College Code of Conduct is based on principles that derive from the nature of the College as a Christian institution: biblical concepts of love and respect for individuals, property and the environment. It is expected that the behaviour of all members of the College community will reflect these concepts and all members will try to live in a manner that pleases God.

7.2 The Code of Conduct applies to students and staff of the College at all times and in all places during the period of their registration or employment with the College, including vacations. It is expected therefore that all members of the College community will:

a. function within the framework of the College as a Christian institution;
b. demonstrate love, with related virtues of respect and consideration, for others, both inside and outside of the College community;
c. act justly, fairly and honourably as an expression of their commitment to the College community;
d. adopt a diligent and co-operative approach to all aspects of academic life;
e. take responsibility for the creation and maintenance of a supportive educational community in which everyone can self-manage their learning and teaching;
f. demonstrate commitment to College life and activities;
g. maintain the good name of the College.

7.3 The following are examples of conduct which are not acceptable to the College community, and which may lead to the invoking of the relevant disciplinary procedure (or, if appropriate, contact with the police):

7.3.1 **Disciplinary offences** including but not limited to:

a. Activity which brings the College into disrepute;
b. Misconduct in relation to the use of any of the College facilities, services and accommodation;
c. Disruption of the normal operation of activities within the College;
d. Harassment or misbehaviour on College property or in dealings with others;
e. Provided that this schedule of offences does not infringe the legitimate right of students to assemble and express grievances.

7.3.2 **Minor Offences** or mild infringements are all those actions which could cause minor offence to the College and its members.

7.3.3 **Major Offences** or serious infringements include:

a. Conduct which does or is liable to cause, violence to a person or damage to property. Please note that exercising freedom of speech or academic freedom, no-one is permitted to commit acts of violence or terrorism.
b. Majorly interfering with, or unreasonably impeding members of the College in carrying out their duties.

c. Bribery, theft, fraud or misapplication in connection with funds or property of any kind in College.

d. False pretences or impersonation of others, within or without the College, in connection with academic attainments or financial awards (this would be dealt with under the College **'Academic Misconduct Policy'**).

e. Refusal or failure to pay a fine or comply with any penalty (subject to any right of appeal applicable) imposed by the College.

f. All forms of bullying and harassment, including sexual and racial harassment, in all College locations and situations where students are participating in formal College activities or are representing the College or are present at events, social or otherwise, organised in association with the College. If this has been alleged, please see the College **'Harassment Policy'**) for added information.

g. Victimisation or retaliation of a student or staff member or employee who has, in good faith, made, supported or assisted in the making of a complaint – even if the complaint is not upheld – provided the action was taken in good faith.

h. Misuse of e-mail, social media, computer facilities, or any aspects of College communications networks.

i. Dishonesty in relation to dealings with the College, its staff members, visitors and associates and other students.

j. Actions which may be injurious to the health, safety and welfare of any person.

k. Moral misconduct as defined by the College's Doctrinal Statement and the Biblical teaching referred to therein.

8 COLLEGE ACCEPTABLE USE OF ICT

The following rules specifically apply particularly to the use of the College ICT facilities and should be adhered to by all users. The scope of these rules will vary with time as new technologies and new social trends develop:

8.1 **Copyright:** Users may not use College property, networks or services to break copyright laws – e.g. downloading, using or distributing software without legally obtained licences where required. All emails, files and materials produced by College staff in the course of their work are the property of College, not the staff who produce them. This means, for example, that deleting emails / files when resigning from work would constitute a deliberate destruction of College property. See also 10.1.1 and 10.1.2 below.

8.2 **Confidentiality and privacy:** Users should respect the ownership of information. Revealing information to anyone not authorised to access that information is prohibited. Users must not access sites and services to which they are not entitled – this includes accessing other people's email, using other people's passwords, hacking into websites of other organisations, etc. Exceptions to this are where, to ensure the smooth operation of College business, it is necessary to monitor or otherwise use another staff member's emails, (for example, because of absence, and this would normally be with the express permission of the staff member).

The College respects the privacy of all users; however, they should be aware that data may be viewed by members of the ICT Team. Such monitoring is necessary in order to ensure the acceptable and effective use of College ICT systems and services.

8.3 **Personal usage:** It is recognised that users, on occasion, need to spend a proportion of their time on "non-work" or academic matters. This can help with personal, and professional, development, which is in line with the ideals of the College. It is also recognised that for students, College is their home and that ICT forms a key source of communication and relaxation. However, the following should be avoided:

a. As far as possible, personal phone calls, Skype chats and internet browsing should be carried out during scheduled breaks and for students outside of timetabled study and class time.

b. Transferring large amounts of personal data should be avoided, particularly during office hours.

c. Storing personal files on College systems (videos, photos, music etc.) is not permitted and alternative storage solutions should be adopted.

d. College email addresses should not be used for personal gain e.g. for personal subscriptions, orders etc.

e. Personal portable devices (phones, laptops, etc.) should only be connected to College networks by staff with the permission of the IT Assistant responsible for the system concerned. (See also **Portable Devices Policy** and on condition that they do not interfere with the user's work or with normal College operations at any time.

f. Users are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, they should consult their line manager.

9 COLLEGE UNACCEPTABLE USE OF ICT

9.1 The activities itemised below are not exhaustive but attempt to provide a framework for activities that fall into the category of unacceptable use. Other activities that are in breach of the Code of Conduct (section 7) may also be deemed to be unacceptable.

9.2 The following activities are strictly prohibited, unless the exceptions mentioned in 9.3 apply:

9.2.1 System and Network Activities

a. Under no circumstances should College ICT system or network be used to engage in any activity that is illegal under English, European or international law.

b. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by College.

c. Unauthorized copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the College or the end user does not have an active license without the authorisation of the ICT Manager.

d. Exporting software, technical information, encryption software or technology, in violation of national export control laws. The appropriate management should be consulted prior to export of any material that is in question.

e. Deliberate introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, and other malicious code) or engaging in any other activities that may, or are intended to, corrupt or destroy other people's data and/or disrupt their use of the College's ICT facilities.

f. Deliberate failure to take sufficient precautions to prevent the transmission of viruses and other malware when using the Colleges ICT facilities.

g. Revealing passwords to others or allowing use of your personal network profile by others. This includes family and other household members.

h. Accessing, transmitting, downloading or storing material that is, or could be deemed to be discriminatory, defamatory, harassing, insulting, offensive, pornographic, obscene, excessively violent or otherwise may cause self-harm or harm to others.

i. Making fraudulent offers of products, items, or services originating from any College account.

j. Causing security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that they not expressly authorised to access. For the purposes of this section, “disruption” includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

k. Port scanning, or security scanning, is expressly prohibited unless prior permission from ICT staff is received.

l. Executing any form of network monitoring which will intercept data not intended for the user’s device, unless this activity is a part of a member of staff’s normal duties.

m. Circumventing user authentication or security of any device, network or account.

n. Providing information about, or lists of, College students, staff, volunteers, voluntary workers or other individuals connected with the College unless it is a part of duties authorised by their Line Manager or the Senior Leadership Team.

9.2.2 Email and Communications Activities

a. These activities are reiterated and expanded upon in the College’s Email Communication Services Policy.

b. Sending unsolicited email messages, including the sending of “junk mail” or commercial or advertising material of any kind (Spam).

c. Any form of harassment via email, telephone, texting or blogging, whether through language, frequency, or size of messages.

d. Unauthorized use, or forging, of email header and footer information.

e. Creating or forwarding “chain letters”, or “pyramid” schemes of any type.

f. Deliberately failing to take due care for others’ privacy and security when using College ICT facilities for email and other communication.

g. Engaging in any blogging or posting on social media that may harm or tarnish the image, reputation and/or goodwill of College and/or any of its employees, volunteers, voluntary workers, partners or clients. This includes making any discriminatory, disparaging, defamatory, sexual or harassing comments or otherwise engaging in conduct prohibited by any other College policy.

h. Attributing personal statements, opinions or beliefs to College on blogs, or any form of social media. Users assume responsibility for any and all risk associated with blogging and using social media.

i. The College trademarks, logos and any other intellectual property belonging to or used by College shall not be used in connection with any blogging activity or social media unless this is required in the course of duties authorised by the line manager or Senior Leadership Team.

9.3 Exemptions

9.3.1 Some users may be exempted from some of the above restrictions during the course of their legitimate job responsibilities – these exemptions will be made clear by the job description and/or by their line manager.

9.3.2 Students and staff wishing to conduct legitimate academic research involving the accessing of sensitive material may also be exempt. However before accessing such material, they must complete the Research Ethical Procedures and comply with the **Research Ethics Policy**.

10 COMPLAINTS

10.1 Should a user wish to raise a concern about acceptable and unacceptable use 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.

10.2 If the user is still unhappy with the level of service provided, they should complain using the College **Complaints Policy**.

11 DISCIPLINARY PROCEDURES

11.1 The College hopes that all users will enjoy studying/working and using the facilities at the College and that they will observe the rules and standards for ICT use and general behaviour that have been set out in this policy and the College Code of Conduct. However, in the event of a failure to do so, disciplinary measures will be taken and in certain circumstances other statutory bodies informed.

11.2 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).

11.3 The College reserves the right to restrict or block a particular user's network or internet access to prevent unacceptable use, and to remove or amend any files or information stored on the network or posted on the College's social networking sites and website.

11.4 Accusations of misconduct by:

- **Students:** will be investigated in accordance with the **'Conduct, Conflict and Student Disciplinary Policy and Procedure'.**
- **Staff, including Voluntary Workers:** will be investigated using the College **'Staff Disciplinary Policy and Procedure'** document, which is available from the College Administrator.
- **Volunteers** will be investigated by the College Administrator in discussion with the Senior Management Team.
- **External Library Users:** will be investigated within 14 days by the Information and Learning Services Manager in discussion with the Librarian, and Senior Leadership Team.
- **Conference Delegates:** will be investigated within 48 hours by the Conference Manager in discussion with the Senior Leadership Team.

11.5 The college is committed to considering all disciplinary cases fairly. The College makes every effort, in accordance with its **'Equal Opportunities 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.

11.6 All disciplinary case records are kept in accordance with the Data Protection Act 2018. See the All Nations Christian College **Data Protection Policy** for details, which includes details of data subject rights regarding the handling of their data.

12 ROLES, RESPONSIBILITIES, POLICY APPROVAL AND REVIEW

12.1 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 use of 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.

12.2 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 use of 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.

12.3 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 complaints brought under the terms of this policy in line with the College Complaint's 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.

12.4 The ICT Manager is responsible for:

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

12.5 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.

12.6 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.

12.7 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 ICT responsibly, safely and with due consideration for others
  - discouraging others from any form of inappropriate use of ICT by making it clear to others that such behaviour is unacceptable
  - supporting anyone who either 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.

12.8 **College and Recruitment and Training Administrators** have a responsibility to manage the administration of the complaints and appeals processes.

13 POLICY COMMUNICATION

13.1 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.

13.2 The '**Staff Disciplinary Procedure'** can be found in the Staff Handbook Appendices which is obtainable from the College Administrator.

13.3 Every effort will be made to respond to any request to provide this policy in a different format.

13.4 This policy will be included in staff and student induction.

14 RELATED DOCUMENTS

The following College documents are related to this policy:

- All Nations Christian College Code of Conduct,
- 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 Equal Opportunities and Diversity Policy
- All Nations Christian College Data Protection Policy
- All Nations Christian College Harassment Policy
- All Nations Christian College Complaints and Policy and Procedure