ACCEPTABLE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) POLICY AND PROCEDURES 2023-24

Document Title		
ACCEPTABLE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) POLICY AND PROCEDURES		
Document Author and Department:	**Responsible Person and Department:**	
ICT Manager	Head of Operations and ICT Manager	
Approving Body:	**Date of Approval:**	
Senior Leadership Team	20.09.23	
Date coming into force:	**Review Date:**	**Edition No:**
21.09.2023	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 Acceptable Use of Information and Communications Technology (ICT) at All Nations Christian College including those validated by The Open University.

July 23: All ICT related policies have been reviewed and amended so that:

- All acceptable and unacceptable use of College ICT facilities are now listed in Appendix A of this policy. (Except those strictly relating to staff and their use of personal portable devices, which are included in that Staff policy)
- The Roles and Responsibilities section is now incorporated in the ICT General Policy only.
- The Legislative Framework section has been updated
- Amendments have been made to typography, grammar, changes to job titles, document names and hyperlinks have been updated (and track changes accepted).
- The order of policy sections has been altered where it makes sense to do so.

Specific amendments to this policy are listed here (NB identified by new paragraph location):

- 4.2, added '*printers/copiers'*
- 7 new wording at end of paragraph now that list of acceptable use has moved to App'x A
- 8, Code of Conduct replaced with link to policies concerned
- 11, addition of reference to appeals.

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) are 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

Legislation which covers the correct use of ICT includes, but is not confined to, the following:

- **Human Rights Act 1998**, which states individuals have a right to respect for the privacy of their communications.
- **Data Protection Act 2018** and the **UK General Data Protection Regulation**, covers the rights of data subjects, data processors and data controllers.
- **Investigatory Powers Act 2016** which covers any monitoring or investigations e.g. tracing network faults or policing acceptable use etc.
- **The Computer Misuse Act 1990** which relates to unauthorised access to personal information(including hacking)
- **The Malicious Communications Act 1988, The Harassment Act 2, The Sexual Offences Act 2003, The Criminal Justice and Police Act 2001**, **The Equality Act 2010, The Counter-Terrorism Act 2015, The Copyright, Designs and Patents Act 1988** and **The Digital Millennium Copyright Act 1988** cover different aspects of the use of ICT for criminal purposes.

4 SCOPE

4.1 College is committed to protecting its employees, volunteers, voluntary workers, partners, clients, students 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 to any network, or system, owned or leased by the College (including but not limited to computer equipment, printer/copiers, telephone, 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 sign the declaration in Appendix B, agreeing 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 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.
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).

6 CONFIDENTIALITY AND PRIVACY

6.1 The College respects the privacy of all users; however, users 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.

6.2 Users should respect the privacy of others at all times. This includes not accessing or revealing any information to which they are not entitled to either access or share with others.

7 ACCEPTABLE AND UNACCEPTABLE USE OF COLLEGE ICT FACILITIES

7.1 Acceptable Use

7.1.1 Acceptable use is the use of College ICT equipment, systems and networks to support the carrying out the College's charitable objectives (including training, administration and operations (including trading activities)) or any other permitted activity highlighted by this policy. Limited personal usage is permitted as long as this meets the criteria in Personal Use of College ICT Equipment, Systems and Networks.

7.1.2 Usage is acceptable when:

- it is in support of the College's charitable objectives and is consistent with College policies;
- it is in support of a user's approved job description/duties/studies;
- it is consistent with the College's policy, procedure and guidance appropriate to any system or network being used/accessed;
- the handling of any information is appropriate for the type of information; and
- limited personal use meets the criteria as defined in Personal Use of College ICT Equipment, Systems and Networks.

7.1.3 Any questions or guidance about acceptable usage should be discussed with the ICT Manager. A more detailed (but non-exhaustive list of acceptable use of ICT can be found in Appendix A)

7.2 Personal Use of College ICT Equipment, Systems and Networks

7.2.1 ICT equipment and services may be used for limited personal usage provided tha

- this is not associated with monetary reward;
- it is undertaken in the user's own time (non-work hours e.g. lunch break,
- before or after work);
- it does not interfere with the delivery of the College's charitable objectives or the user's proficiency in fulfilling the requirements of their job description/duties/studies;
- it does not violate this or any other College policy;
- it is a lawful activity that does not contradict the relevant Code of Conduct

7.2.2 Whether using College ICT facilities for College or personal use, all users must abide by Appendix A of this policy at all times. They must also agree to do so by signing the declaration in Appendix B

7.3 Unacceptable use

7.3.1 Users must only use ICT equipment, systems or networks that have been authorised for their use.

7.3.2 Unacceptable use would include:

- any attempt to gain unauthorised access to any ICT equipment, systems or networks provided by the College;
- use of the College's ICT equipment, systems or networks to gain unauthorised access to any other system; or
- any use of College ICT equipment, systems or networks which does not uphold the principles of acceptable use as outlined in this policy.

7.3.3 Any such use may be a breach of this policy, and may also be a breach of legislation (including the Computer Misuse Act 1990). A more detailed (but non-exhaustive list of unacceptable use of ICT can be found in Appendix A) (based on Aberdeen City Council [1]

8 COLLEGE GENERAL CODE OF CONDUCT

8.1 This policy is embedded within the terms of the College's Code of Conduct.

8.2 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.

8.3 The Student Disciplinary Policy and the Staff Disciplinary Policy both contain a Code of Conduct. These apply at all times and in all places during the period of a person's registration or employment with the College, including during vacation periods.

9 DISCIPLINARY PROCEDURES

9.1 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 may be taken.

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).

9.3 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.

---

[1] https://peopleanytime.aberdeencity.gov.uk/wp-content/uploads/2017/11/ICT-Acceptable-Use.pdf)

9.4 Accusations made by anyone concerning misconduct by:

- **Students:** will be investigated in accordance with the Student Disciplinary Policy **.**
- **Staff, including Voluntary Workers:** will be investigated using the College Staff Disciplinary Policy which can be found in the Additional Staff Policies & Procedures on the P Drive and is also obtainable from the HR Lead.
- **Volunteers** will be investigated by the HR Lead in discussion with the Senior Leadership Team.
- **External Library Users:** will be investigated within 14 days by the Head of Learning Services 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.

10 COMPLAINTS AND APPEALS

10.1 Should a user wish to raise a concern about College ICT services which they should reasonably expect to have received or the acceptable use or misuse of such services, 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 prefer or they are still dissatisfied, they should formally complain using the form at the back of the College Complaints Policy. This policy also includes details of the appeal procedures available following the outcome of a complaint.

10.2 The college is committed to considering all disciplinary and complaint cases fairly and in accordance with its Equality and Diversity Policy and will handle and store such case records in accordance with its Data Protection Policy.

11 ROLES, RESPONSIBILITIES, POLICY APPROVAL AND REVIEW

This section, which applies to all ICT related policies, can be found in section 9 of the Information and Communications Technology (ICT) General Policy

12 POLICY COMMUNICATION

12.1 This policy and any other policies referred to in this document relating to students can be found here. Those relating to staff can be found in the Additional Staff Policies & Procedures on the P Drive and is also obtainable from the HR Lead.

12.2 The General 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

12.3 This policy will be included in staff and student inductions.

13 RELATED DOCUMENTS

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

- Information and Communications Technology (ICT) General Policy
- Email Services Communications Policy
- Social Media Policy
- College staff and volunteers must also comply with the Staff Personal Portable Devices Policy

13.2 The following College documents are related to this policy:

- All Nations Christian College Campus Access Student Handbook
- All Nations Christian College Remote Access Student Handbook
- All Nations Christian College Bullying, Harassment and Sexual Misconduct Policy
- All Nations Christian College Complaints Policy
- All Nations Christian College Student Disciplinary Policy
- All Nations Christian College Research Ethics Policy
- All Nations Christian College Equality and Diversity Policy
- All Nations Christian College Data Protection Policy

APPENDIX A

LIST OF ACCEPTABLE AND UNACCEPTABLE USE OF ICT

All those who use College ICT facilities including College emails or College social media channels are required to agree to comply with the following:

1. SECURITY

i. STAFF

- When using personal portable devices **staff** must follow the Staff Portable Devices Policy and particularly:
  - take all reasonable measures to protect College data stored on the device (including College provided email) from being accessed, hacked, lost, corrupted, or damaged by unauthorised user/s.
  - Agree to not store College data permanently on the device
  - Agree to ensure all College applications and College owned data (including email) are permanently removed, deleted or destroyed before disposing of any devices that have been used for College business.
- Staff must use a secure paying mechanism if using College cards online. They should look for a padlock at the top or bottom of the web page (clicking padlock will confirm secure status) and not divulge confirmation of login details or account information in an email or any other message.

ii. **STAFF AND STUDENTS** should maintain security at all times by ensuring:

a. **Passwords**:
   - are strong (i.e. 12 characters minimum with a mixture of upper and lower case letters, numbers and non-alpha numeric symbols)
   - passcodes and PINS are kept secure
   - where personal devices are used to access College emails, the device itself is protected with a strong password and/or fingerprint/facial recognition
   - are never shared with another person or used for any other purpose
   - are changed immediately when it has become known by a third party.

b. **Devices** are protected by strong passwords and all reasonable measures are taken to protect College data (including College emails) from being accessed, hacked, lost, corrupted or damaged by unauthorised user/s.

c. **Email** access:
   - is only from a suitably safe and strong password protected computer/device (e.g. mobile phone, tablet, laptop or home computer)
   - limited to legitimate users i.e. no other person is able to view College emails
   - reported to the ICT department when there are any concerns that a device or an email is unsafe.

d. **Action is taken when fraudulent emails are suspected:**
College staff frequently receive malicious emails. Where this happens to any user, they should:
   - Delete objectionable emails immediately using shift-delete, which deletes the message without retaining a copy.
   - Train themselves to be suspicious of any email that raises the slightest concern for whatever reason.
   - Always check carefully that the sender's email address is genuine

- Beware malicious emails which appear at first glance to be valid. (For example, staff may receive a simple request for help apparently from another member of staff or a request for a payment authorisation or a request to click on a link).
- Verify a suspicious email that appears to come from someone you know by contacting them through a different means, such as a phone call or text. Alternatively forward the email to the ICT support team.
- Think before you open an attachment or click on a link since both can be used to propagate malicious software. Ask yourself: “Do I know the person?” “Is the sending email address legitimate?” “Does the subject line make sense?” Rather than click on a link, copy and paste the link into the Notepad App and see where it would take you.

e. The IT Department is informed promptly:

- when an email password has become known to a third party,
- when you suspect a virus or malware has been released onto the College network,
- when College ICT facilities are damaged, faulty, stolen or lost,
- if you become aware of a third party breaching the College policy on Acceptable Use of ICT Facilities.

f. The College is informed promptly:

- If a complaint is made on the College's social media channels, advice should be sought from the Director of Communications and the Compliance Officer before responding. If they are not available, then you should speak to the Head of Operations or the Principal.
- Sometimes issues can arise on social media which can escalate into a crisis situation because they are sensitive or risk serious damage to the College’s reputation. Examples might include the College’s position on sexual ethics. The nature of social media means that complaints are visible and can escalate quickly. Not acting can be detrimental to the College.

2. PRIVACY

Particular care should be taken with personal data (as defined by UK GDPR 2018) accessed via ICT systems. Users should ensure:

- You do not violate the privacy or safety of others, particularly by disclosing information or images of those who may be at risk if their names or images are posted online. Disclosing information/images about other members of the College on the internet without their explicit consent is strictly forbidden.
- Any information about living individuals is held in accordance with the College Data Protection Policy.
- Such data is deleted immediately after use or transferred to secure storage with limited access.
- any personal, commercially sensitive or restricted information to which you gain access in using College ICT facilities must be treated as confidential. 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.

3. EMAIL AUTHORISED USES

The main purpose in providing email is to support the teaching, learning, research, and administrative, operational and business activities of the College. Users who have been provided with access to College emails are responsible for all emails originating from their account. Therefore, you must understand that:

- All emails relating to College business must be sent using the College email services.

- Emails sent from College email addresses will be perceived as being official communications, and professional language should be used at all times.
- College email services should normally only be used for College business. However:
    a. students may also use their College email address with appropriate student discount web sites (e.g. Unidays).
    b. members of staff (including Associate Lecturers and volunteers) who have a legitimate reason for using their College email for personal business, should discuss this with the Principal/CEO and ICT Manager before doing so.
- College student email addresses are to be used for contact between the College and students for communicating and collaborating effectively during the course of their studies.
- Student Microsoft 365 accounts, including email, are provided at the discretion of the College and are deleted within 4 months of the student ending their course of study.

4. UNAUTHORISED USES OF COLLEGE ICT FACILITIES [2]

The use of College ICT facilities including College emails or College social media channels should not be abused. An absolute definition of abuse is difficult to achieve but certainly includes (but is not necessarily limited to) the following:

- Using College ICT facilities without permission. This includes using computers, telephones and networks, or accessing, copying, reading, or storing software, databases, messages or data. You must not attempt to gain unauthorised access to any College ICT facilities, or use College facilities to gain unauthorised access to other ICT facilities.
- Using College email addresses for personal correspondence or other personal use (for exceptions see authorised uses above).
- (Staff only) Downloading College emails onto a personal device without the appropriate permission. See the Staff Personal Portable Devices Policy.
- Using College ICT 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.
- Deliberately failing to take due care for others' privacy and security when using College ICT facilities for email and other communication. This includes revealing information to anyone not authorised to access that information.
- Deliberately circumventing any controls imposed by the College on the use of its ICT facilities.
- Knowingly downloading, transmitting, storing, generating or using any programme, tool or virus designed to damage or disrupt or in any other way interfere with the functioning of ICT 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.
- Creation or transmission of material which brings the College into disrepute. This includes engaging in any blogging or posting on social media that may harm or tarnish the image, reputation and/or goodwill of the College and/or any of its members.
- Using the College trademarks, logos and any other intellectual property belonging to or used by College without permission and attributing personal statements, opinions or beliefs to the College on blogs or any form of social media.
- Creation or transmission of material on social media without reference to the guidelines in the College Social Media policy. When representing the College on social media, care should be taken with: presentation (grammar, quality of images etc), accuracy (facts should be checked),

[2] https://www.bath.ac.uk/corporate-information/email-policy/ (Acceptable use)

tone (consider carefully before posting), honesty (if you have made a mistake, admit it), clarity (to distinguish between your personal opinion and those of the College), legal (e.g. not using unauthorised footage), avoiding contentious issues (let the Communications and Fundraising Team handle these) and safe (care when revealing personal information).

- Creation or transmission of material that is illegal under English or International Law.
- The transmission of unsolicited commercial or advertising material, chain letters, press releases or other junk-mail of any kind.
- The unauthorised transmission to a third party of confidential material concerning the activities of the College.
- The transmission of material such that this abuses the ownership of the information and infringes the copyright of another person or entity protected by copyright, trade secret, patent, other intellectual property or similar laws or regulations.
- Using software without a license agreement 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.
- Activities that unreasonably waste network resources e.g. Filling a mail box with videos, photos or other material which require high storage capacity.
- Activities that corrupt or destroy other users' data or disrupt the work of other users.
- Activities which cause damage to College-owned ICT facilities, or moving or removing such facilities without authorisation.
- Creation, transmission, storage, downloading or displaying of any offensive, obscene or indecent images, data or other material (See the Research Ethics Policy for the limited permissible use of such material for academic purposes).
- Creation or transmission of material which is designed or likely to cause annoyance, inconvenience or anxiety.
- Creation or transmission of material that is abusive or threatening to others, serves to harass or bully others, discriminates or encourages discrimination.
- Creation or transmission of defamatory material or material that includes claims of a deceptive nature.
- Activities that violate the privacy of others or unfairly criticise, misrepresent others; this includes copying distribution to other individuals.
- Creation or transmission of anonymous messages or deliberately forging messages or email header information, (i.e. without clear identification of the sender) or for being insulting or offensive.
- The unauthorised provision of access to College services, systems and facilities by third parties including, but not limited to, revealing login details and passwords to others or circumventing user authentication or security of any device, network or account.
- The use of ICT to infringe any other College regulation, including the Code of Conduct.

5. ON LEAVING COLLEGE

The College is the owner of all College information, the contents of all College systems, everything which is created on, transmitted to, received on, printed from, stored or recorded on each device, irrespective of who owns the device, where it is used in the course of College business or on behalf of the College.

College owned data should be deleted from personal devices when staff end their employment or students leave the College. Therefore, you are required to agree:

- not to store College data permanently on a personal device.

- to ensure all College applications and data (including email, teaching materials, copyrighted materials etc.) are permanently removed and deleted when leaving College and permanently removed, deleted or destroyed before disposing of any devices that have been used for College business or purposes.

APPENDIX B

ALL NATIONS CHRISTIAN COLLEGE

ACCEPTABLE USE OF ICT DECLARATION

Name:

I confirm that I have read and agree to comply with this policy, and in particular the obligations of Appendix A, whilst a student or member of staff at All Nations Christian College.

I further declare that I will not disclose any personal information about other students or staff of All Nations Christian College on any website or social network, without their explicit consent. This includes their names, pictures of them, dates of birth, or any other information about their identity.

I recognise that by disclosing information on the Internet, I might put other students or staff at risk in the future.

Signature:

Date: