ICT ACCEPTABLE USE POLICY

CATEGORY	**Audit & Risk**
POLICY OWNER	**Director of Operations & Sustainability**
DATE & VERSION	**15th September 2023 - Version 3.1**
APPROVED BY	**Audit & Risk Committee**
REVIEW FREQUENCY	**Annual**

Contents

1. **Policy Purpose**

   UWC Atlantic (the College) has a diverse set of ICT facilities, which we hope you will use and benefit from. This policy sets out the College's expectations that you must comply with to ensure that the system works effectively for everyone.

2. **Policy Statement**

   The College must meet the requirements of all applicable UK laws relating to the use of computers or the protection of data and copyright. These laws include (but are not limited to):

   - Data Protection Act (DPA 2018)
   - Privacy and Electronic Communications Regulations
   - Copyright, Designs & Patents Act, 1988
   - Obscene Publications Act, 1959
   - Computer Misuse Act 1990
   - Defamation Act, 2013
   - Criminal Justice and Immigration Act 2008
   - Digital Economy Act 2017

   This policy applies to all individuals who are provided with a UWC Atlantic network account, whether employees, student, board member, volunteer or any other category of account user.

3. **Policy Implementation**

   3.1 **Privacy**

   The College will respect your privacy on the ICT systems, where it is possible to do so. However, under some circumstances it may be necessary for ICT or senior College employees to view the data stored by you. We will only do so if it is necessary to resolve a fault, ensure proper operation of ICT facilities, investigate misuse or another disciplinary matter, or on wellbeing or safeguarding concerns, and if practical and whenever possible we will attempt to contact you to seek permission first. We may on occasion be required to disclose information to third parties, such as the Police, without needing to obtain your consent.

   In using the College's ICT systems you consent to the viewing or disclosure of data resulting from your use of our systems.

   3.2 **Support**

The ICT Team will support the use of the College's ICT Systems. Please report all faults or malfunctions to the ICT Team as soon as possible. If there are multiple issues to be dealt with, they will be addressed in the following general order of priority:

- Core server operation, tasks related to continued operation of core services and disaster recovery, including urgent patching or security functions.
- Issues that affect key administrative functions or important teaching that has a time constraint.
- Issues relating to core user applications, such as iSAMS, MyConcern and Breathe, internet or e-mail use.
- Issues relating to software used by individual departments.
- Upgrade of existing facilities or software.
- Installation of new facilities or software.

We will periodically need to undertake maintenance work on all devices. When this is necessary, please ensure that any devices in your working space are readily accessible. If you have a laptop on which we need to perform maintenance, please respond promptly to a request to bring it in, or contact the ICT Team to arrange a convenient time.

The most effective way to request support is by submitting a ticket through TopDesk which can be found on the College Intranet.

User guidance can be found as follows:

- **Appendix 1 - General Expectations**
- **Appendix 2 - Internet Use**
- **Appendix 3 - E-mail Use**
- **Appendix 4 - Personal Computing Devices and the Wireless Network (Bring Your Own Device)**

3.3 Consequences for misuse of the College ICT systems

If you do not meet the expectations set out in this policy, we may disable your access to some or all of the College ICT systems, either to investigate any misuse or as a disciplinary measure. Measures may include bandwidth or time restriction, banning of devices, additional monitoring procedures, or loss of access altogether.

Serious breaches may result in formal disciplinary action and in the case of illegal acts also be reported to the Police. If you are in any doubt about whether something is

allowed, check with the ICT Department **before** doing it.

4. **Related Information**

4.1 Digital Safety

UWC Atlantic implements appropriate safeguards within the College while supporting employees and students to identify and manage digital safety risks independently and with confidence. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies. Further information can be found in the Digital Safety Policy.

4.2 Data Protection

The College has a responsibility to look after the data it holds, to ensure that it is used appropriately, and that it is accurate and up-to-date.

4.3 Use of Confidential Data

All employees accessing confidential data (including names, addresses, personal details of students and the College email address book) must familiarise themselves with the following:

- UWCA Data Protection Policy
- Data Protection Act 2018 that govern our use of data.

Confidential data will usually be stored and processed only on the College's ICT systems or approved cloud-based platforms. It is expected that most employees would use Remote Access to work on data while at home or away from campus. You must not remove or copy confidential or personal data from the network to personally-owned computers or media (for example via email, cloud storage or on a USB stick) unless you have specific written permission to do so. This includes synchronising the College email address book to a personal device.

Permission to process data away from the College's ICT systems can only be granted by the College Data Controller. If this permission is granted, the following responsibilities apply:

- Data may only be copied to and stored on an approved encrypted device, such as an encrypted USB stick, which can be sourced through the ICT Team, or by other means of encryption to be approved by the ICT Team.

- If the data is to be e-mailed, a suitable encryption method must be used, and be approved by the ICT Team.
- You are solely responsible for ensuring that any personal device you use to work with College data is free of viruses and other malware, and must install appropriate software to ensure your device is malware free.
- You are solely responsible for ensuring that any data you hold is securely disposed of when the purpose for which it is being used has ended.
- You may only manage and communicate personal or confidential data using College accounts (and email accounts). When using cloud-based platforms (e.g. Google's G- Suite) you may only use College-provided accounts to work with confidential and personal data and must not connect to or synchronise with personal accounts.
- All new proposed uses of personal data require a Privacy Impact Assessment to be completed, and permission from the College Data Controller before any work is undertaken.
- Be careful when emailing; only send confidential data to people you know are authorised to see it. Use BCC when sending to lists of external recipients who should not have their personal email addresses revealed. Check when forwarding emails that confidential data is not hidden within the text of earlier replies.
- Minimise printing where possible; only print confidential data when it is absolutely necessary, and dispose of the printed copy securely as soon as it is no longer needed. Keep all printed confidential data secure, in a locked office or cabinet.

If you become aware of or suspect that a loss of confidential data has occurred, you must immediately report this to the College's Data Controller. Potential sources of loss may include such things as losing a device that contains College data or having it stolen, becoming aware that confidential data is being used outside the boundaries of the College network, or finding a virus or malware on a computer you use for working with College data.

Please note that any breach of this policy will result in disciplinary action being taken.

5. **Policy Measurement and Reporting**

The ICT Acceptable Use Policy is reviewed annually by the Audit & Risk Committee of the Board, the Director of Operations and Sustainability and the ICT, Compliance & Risk Manager, as part of the operational review cycle and as part of the whole College

development plan. Part of this review process will consider to what extent the policy is being used as an active working document.

The policy is communicated to the school community electronically on ***Every*** and is available on the UWCA website.

Appendix 1 - General Expectations:

It is the responsibility of all UWC Atlantic Community Members to ensure that:

1. Your User ID (account) and password are for your use only. Do not allow anyone else to use your account and do not use anyone else's. Do not reveal your password to anyone, or write it down, and do not leave your computer logged in while you are away from it.

   We can only support you if we know that you are the only one using your account. All use of the facilities by your User ID will be attributed to you, and you will be held accountable. It is very important that you never pass on to anyone else the details of your account or let them use it, whether or not you are present at the time. The ***only*** exception is for ICT employees, who may ask for access to your account to diagnose a problem.

2. You use a password that cannot easily be guessed, and change it regularly.

3. You log into only one computer at a time. Always log out when you are finished.

   - Not only does logging in to more than one computer prevent other people from using the ICT facilities, it can also cause problems for your User Account.
   - Don't leave a shared computer logged in with the desktop locked. Log out if you are going to be away from the computer for a while.
   - Don't leave your computer logged in overnight. We may need to carry out maintenance on the ICT systems, and you could lose unsaved work if there is a problem or a power cut.

4. Before printing, please check whether you really need to print the document in question, and ensure that you have checked it for errors. You have a quota for printing, and if you run out you can buy more. Don't feel that you have to use up all of your quota.

5. You do not attempt to find or exploit features or flaws in the system which may give access to information or areas not normally available to you. The possession or use of any software or tools designed to test or circumvent network security or to hide your identity is strictly forbidden anywhere on campus or in relation to any of the College's systems. This includes the use of virtual private network (VPN) software.

6. You avoid using the facilities in any way that may cause inconvenience or unnecessary work for anyone else.

7. You do not corrupt or destroy other user's data or violate their privacy.
8. You can use headphone sockets and DVD/CD drives on the College devices, where they are fitted. You may use USB ports on College devices to connect memory storage devices and upload data from stored devices such as cameras and phones. Do not connect any other hardware to College devices without the permission of the ICT Team. Do not disconnect or alter the cable connections on any College ICT equipment.
9. All files and media you bring into the College are undamaged and free of viruses. If a College computer reports the presence of a virus on your media (USB stick, phone, camera) you must report it immediately, and **stop using the infected media.** If you suspect that a College device has a virus, report it to a member of the ICT Team immediately. To avoid the spread of hoax warnings, do not pass on virus warnings to anyone else.
10. When using College devices, you only use the software we have installed for you. You must not attempt to install other software of any kind onto the College's ICT systems.
11. You do not use the College network or internet connection to offer file or software services to other people, whether inside or outside the College.
12. Use only the amount of storage space that is provided for you on the College network. You will need to manage this space by deleting old files when they are no longer needed. If you have a real need for more space, please speak to a member of the ICT Team.
13. Remember that when communicating via the College's ICT system, you are acting as a representative of the College.

    Always act as a good example of the UWC values in your communications.
14. You do not bring food or drink into the ICT rooms.

    Please treat ICT equipment with care and respect, and keep a quiet working atmosphere in the shared ICT areas.

Appendix 2 - Internet Use

The College provides you with access to the internet through the computer network. The internet is a large and very useful source of information. Numerous web sites and services, both official and unofficial, provide information which would be useful for educational purposes. However, there are risks associated with internet use, and the consequences of misuse can impact the whole community. These are the main issues:

- Although the internet is often described as 'free', in fact there is a significant cost to the College for using it. This cost includes connection charges, subscription costs (which may depend on how much a service is used) and the hardware and software needed to support internet access. We must therefore ensure that we are making best use of this expensive resource, and that inappropriate use by individuals does not prevent the rest of the community from enjoying its benefits.
- Although there is much useful information on the internet, there is a great deal more material which is misleading or irrelevant.
- Unfortunately, the internet carries a great deal of unsuitable and offensive material.
- It is important for legal reasons, in respect of UWC values, and to protect the College's employees and students, that access to this unregulated resource is appropriately managed by the College. Accessing certain websites and services and viewing, copying or changing certain material, could amount to a criminal offence and give rise to legal liabilities.
- There is a danger of introducing viruses or other damaging software onto the College's network or passing viruses to a third party.
- Misuse of our internet service can result in legal action, criminal charges, and potentially result in the College losing access to the internet altogether. The internet works in part by co-operation between providers of internet services, and we must be seen to act responsibly.
- An organisation that is found to be a source of viruses, illegal or offensive material may be "blacklisted", and as a result heavily restricted in its use of internet and e-mail services. The College must therefore ensure that its internet and e-mail facilities are used appropriately.
- There are dangers associated with online communication, where it is not always possible

to verify identity or know who is reading messages.

- Be cautious when communicating on-line, and in giving out personal information about yourself or others at UWC Atlantic.
- All websites accessed are recorded, along with the date and time and who accessed them. These records are periodically audited to ensure that our systems are being used appropriately and effectively.
- The College uses software to categorise and where necessary block inappropriate web and e-mail content, in accordance with Department of Education guidelines. If you see any web pages that you believe are incorrectly categorised, please notify the ICT Team.

Any misuse of third party systems or unacceptable use of the internet shall be treated as a breach of the College's Policy and will lead to a disciplinary investigation. Breach of this policy could be deemed to be gross misconduct.

1. Acceptable Use of the Internet

- Research.
- Browsing for information.
- Using online services to which the College has subscribed.
- Personal communication, for example Skype, video-conferencing.
- Leisure purposes provided that the use is occasional and reasonable, does not interfere with your work, and does not prevent another user from performing their work.

2. Unacceptable Use of the Internet

- Creation, transmission or downloading of any offensive or obscene images, data or other material including of a racist, homophobic, violent or extremist nature.
- Creation or transmission of any material which is designed or likely to cause annoyance, inconvenience or needless anxiety, or which is defamatory.
- Excessive use of the available bandwidth (e.g. video or other downloads) especially during the working day.
- Infringement of the copyright of another person.
- Transmission of unsolicited commercial or advertising material, except where the

recipient has agreed to the receipt of such material.

- Deliberate unauthorised access to facilities or services.
- Attempting to bypass any access controls or restrictions on any web site or service.
- Use of “evidence elimination” software or hardware, or use of sites or software designed to disguise the web sites visited. This includes virtual private network (VPN) technology.
- Connection to the internet from the College’s ICT Systems using any other means than that provided.
- Use of file sharing software or services, e.g. torrent software.

Appendix 3 - E-Mail Use

The College's ICT Systems enable students and employees to communicate through email with any individual or organisation with email facilities throughout the world. Like the internet, there are risks associated with email use, and this policy seeks to reduce those risks.

The College will provide you with an email account for your own use. Even if you have your own independent email address, it is important that you check this email account regularly, as your College email address will be used by employees and students to contact you. The following apply to all email users:

- Employees and Governors must use their College email account for all College business.
- While we will respect your privacy where possible, on occasion it may be necessary for ICT employees to view your emails, to investigate a problem.
- If possible, we will discuss this with you beforehand. However, remember that email as a communication medium is not secure, and that anyone on the internet can potentially read the messages you send to and receive from people outside the College. You should never put secret information (such as bank details) in an email.
- All email messages passing through the College's e-mail system are checked for inappropriate content, such as spam or viruses, and blocked if necessary.
- Only open email attachments that you are expecting and are reasonably sure of their content.

The following expectations apply to all email use through the College's ICT systems, regardless of whether email is sent or received through a College or personal email account.

Unacceptable use of e-mail

- Introduction of program files, viruses or other potentially damaging software onto the College's ICT systems, or use of the College's ICT systems to transmit such software.
- This might happen by opening an email attachment or following a link in a message. Although virus detection software is installed, it can never be guaranteed that a virus will be detected before it causes damage, so introducing non-essential software is an unacceptable risk. If you have any reason to suspect that a virus may have entered the College's ICT systems, inform the ICT team immediately.

- Removal or editing of any disclaimer the College may add to outgoing messages.
- Use of email to send offensive or copyright material, chain messages, defamatory, bullying or threatening messages. Sending unsolicited commercial e-mail (spam).
- Sending the same message to multiple people without good reason. Please ask yourself whether everyone you intend to send a message to really needs to receive it.
- Spoofing email information, such as sender address, or the use of an email account for which you are not authorised.

Appendix 4 - Personal Computing Devices and the Wireless Network (Bring Your Own Device)

The College has a wireless network which covers a large proportion of the campus. You are permitted to bring in your own devices (laptops, smart phones, tablets) and connect them to the wireless network.

1. Responsibilities

You may connect your personal devices to the wireless network to gain access to the internet and log-in to your College email account.

If your device switches MAC address as a privacy measure, you will need to turn this feature off, otherwise you will rapidly run out of connections.

You must use your own College user account to log-in to the wireless network. Do not use a device that somebody else has logged in, or allow somebody else to use a device that you have logged in. You may only use the appropriate wireless network assigned to you (AC BYOD - **B**ring **Y**our **O**wn **D**evice). Students and employees should not use guest Wi-Fi codes.

You may only connect devices directly to College access points. You must not share a connection from your device to other devices. You must not connect your personal device to any other part of the fixed College ICT systems. This includes wired data ports and fixed projectors/screens/AV equipment installed in classrooms. You may connect your device to a portable projector or speakers, or to Bluetooth-enabled equipment, where available.

You have the same internet access as you would from a College computer. This access is filtered and logged in the same way, and you have the same responsibilities regarding appropriate use of the internet.

The wireless network is made available primarily for personal research use. You may also use it for leisure use, but please always be aware of the amount of bandwidth you are using, and do not make life difficult for other users. Please remember that the use of file sharing and VPN software is strictly banned.

Support for connecting your personal ICT devices is on a best-endeavours basis. We will try to help with connection problems where possible, but the time we have available is limited.

You are responsible for ensuring that any data on your personal device is backed up.

You are solely responsible for ensuring that any device you use to connect to the College network is free of viruses and other malware. You must install anti-virus software on your device before you connect, and keep it up to date. **This is not optional – if you are unable or unwilling to keep your device free of viruses then do not bring it into College.**

If for any reason your personal device causes a problem, or, in our opinion, poses a potential risk to the College's ICT systems, we reserve the right to stop that device from being connected.

Employees must not use personal devices in the classroom or in other teaching settings. We cannot provide support for the use of personal devices for administrative work.

Personal email addresses or accounts should not be used for College related business.