DIGITAL SAFETY POLICY

CATEGORY	**Audit & Risk**
POLICY OWNER	**Compliance, Risk & ICT Manager**
DATE & VERSION	**25th September 2023 - Version 4.1**
APPROVED BY	**Director of Operations & Sustainability**
REVIEW FREQUENCY	**Every 3 years**

Contents

1. **Policy Purpose**

   The purpose of this policy is to:

   - ensure the safety and wellbeing of our students while using the internet, social media or mobile devices, whether it is in a classroom environment, social environment or an online learning environment.
   - provide employees and volunteers with the overarching principles that guide our approach to online safety.
   - ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

2. **Policy Statement**

   UWC Atlantic (the College) recognises the benefits and opportunities which technology offers to teaching and learning. We provide internet access to all students and employees, and encourage the use of computers in both teaching and learning. However, the accessibility and global nature of the internet and mobile phone technology mean that we are also aware of potential risks and challenges associated with such use. We want you to be safe online, your data needs to be safe and your relationships need to be safe.

   The ongoing approach of the College is to implement appropriate safeguards within the College while supporting students and employees to identify and manage risks independently and with confidence.

   The policy statement applies to all employees, volunteers, students, contractors and anyone involved in UWC Atlantic's activities. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies.

3. **Policy Implementation**

   The UWC Atlantic Community should ensure it has understood and put into practice the following policies which relate to digital safety:

   - Safeguarding and Respectful Community Policy
   - ICT Acceptable Use Policy

The *Safeguarding and Respectful Community Policy* covers:

- UWC Atlantic's commitment to safeguard all members of the College Community and to protect them from harassment, sexual misconduct, bullying, abuse, assault,

violence or discrimination of any kind.

- All communications and interactions that take place online (as well as in person).
- The Preventative Action taken by the College.
- Roles and Responsibilities for Safeguarding within the College.
- How to report any signs, incidents, concerns or 'nagging doubts' to the Designated Safeguarding Person (DSP or in their absence the Deputy Designated Safeguarding Person) immediately.
- Confidentiality.

The *ICT Acceptable Use Policy* covers:

- Expectations for the use of UWC Atlantic ICT facilities, College network accounts, internet, email, personal devices and the wireless network.
- ICT and the Law.
- Privacy.
- Data Protection and personal information.

The College is registered with the Information Commissioner and complies with appropriate legislative and regulatory standards for data protection as a consequence.

3.1 Security Measures

The ICT Team at UWC Atlantic will make sure that the College network is safe and secure and will keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of College systems and information. Digital communications, including email and internet postings, over the College network, will be monitored by the ICT Team. Further information can be found in the ICT Acceptable Use Policy.

Guidance and advice including online behaviour can be found at **Appendix 1 - Guidance and Advice**

3.2 Reporting Concerns

Any concerns or incidents should be reported immediately to the Designated Safeguarding Person (DSP) or in their absence the Deputy Designated Safeguarding Person (DDSP). The DSP will take prompt and appropriate action in accordance with the procedures outlined in the Safeguarding and Respectful Community Policy

4. Related Information

4.1 Support

Further information, explanation and advice on Safeguarding and the Safeguarding and Respectful Community Policy can be obtained from the Designated Safeguarding Person.

Further information, explanation and advice on using Social Media can be obtained from the Communication and Marketing Team.

Further information on using the College's ICT systems and the ICT Acceptable Use Policy can be obtained from the College ICT Team.

4.2 Relevant Employees

Designated Safeguarding Person (DSP):
Lucretia Fields, VP - Student Life
Email: safeguarding@uwcatlantic.org

Deputy Designated Safeguarding Persons (DDSP)
Chris Blackwell, Clinical Psychologist
Sam Willis, Head of Residential Life
Laura Earwood, Head of Year
Maite Sandoval-Inglada, Head of Year
Email: safeguarding@uwcatlantic.org

College Communications Team, Email: communications@uwcatlantic.org
College ICT Team, Email: staff.it@uwcatlantic.org

4.3 Education and Training

Students receive information about digital safety in the student handbook, during the Induction Period when they first arrive and during a Wellbeing session in the first term of every school year.

Additional guidance can be sought from the Learning Support teams. Issues associated with digital safety apply across the curriculum and within classes students will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

Employees receive information about digital safety as part of their safeguarding training.

5. **Policy Measurement and Reporting**

   The Digital Safety Policy is reviewed every 3 years by the Audit & Risk Committee of the Board and the Director of Operations & Sustainability, 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 - Guidance and Advice

1. Safe and Social

Digital safety applies to all use of the internet and all forms of electronic communication such as email, mobile phones and social media sites. It also applies to online learning.

All members of the UWC Atlantic Community will take responsibility and be accountable for their online presence and how that impacts upon them personally, the people around them and the College.

1.1 Positive Behaviours Online

All members of the UWC Atlantic Community will act positively online and:

- Commit to the UWC values and follow the UWC Common Code of Conduct in action and spirit.
- Consider how you speak to a person online, if you wouldn't speak to the person in that way face to face, then it is also not appropriate online.
- Respect a person's right to privacy and seek permission before you post anything about other individuals or groups within the College. Check that other individuals are happy with you posting a photo of them.
- Avoid posting when you are experiencing heightened emotions. Posting in a moment of anger or frustration for example, can cause you to act without thinking through the consequences. If it helps you, speak with a friend or colleague to discuss your concerns.
- Remember that people you meet in chat rooms may not be who they claim to be - they may be of a different age, gender and personality from those claimed and might have ulterior motives for engaging in chatting with you.
- Never arrange to meet someone alone that you have met over the internet.
- Avoid sharing personal information (including your address, phone numbers, date of birth), your specific location, your schedule or images of yourself or friends online. Everyone is vulnerable to online predators and identity thieves.
- Delete and/or report emails requesting details of passwords (especially for sensitive information such as bank details). These are certainly 'phishing'. They can be reported to the organisation from which they seem to have come from.
- Use different usernames and passwords for maximum protection.
- Make your profiles private, always check your settings. Remember that if you have published it, it's traceable. You cannot rely completely on Privacy Settings, even if your

profile is set to private, a friend could for example download, save or share what you have published.

- Review your accounts regularly. Check the information and content that is accessible on your social media profiles. Locate and remove photos and posts that aren't quite as you intended them to be.
- Google yourself to see what comes up. Edit and delete anything you now consider inappropriate.
- Choose the websites you view carefully. Not all websites are safe. Many encourage viewing but might contain programs (e.g. viruses) harmful to personal or College computers.
- Avoid inappropriate email addresses or hashtags.

1.2 Unacceptable Behaviour Online

All members of the UWC Atlantic Community understand that the following behaviour is unacceptable:

- Cyber bullying
- Negative, aggressive, threatening or hateful posts.
- Posts about other individuals or groups within the College without their permission.
- Posts about any illegal activities. This includes for example: illegal drugs, underage drinking, stealing, damaging property, violence motivated by hate or extreme prejudice etc
- Viewing websites encouraging negative, aggressive and threatening behaviour or unlawful and harmful activities.
- Sharing anything that is sexually explicit.
- Viewing of pornographic material.
- On-line gambling.

1.3 Cyber Bullying

Cyber-bullying includes any form of behaviour designed to hurt, offend or cause distress to other people using any form of electronic communication.

This includes text messages, images or emails by mobile phone or computer.

Comments made on any social network site or website that hurt, offend or cause distress are also considered to be forms of cyber-bullying.

If anyone feels that they are the target of cyber-bullying they should report this immediately and keep any evidence; the advice:

STOP

BLOCK and

TELL

is good when cyber-bullying occurs. Note that it is the perception of the alleged victim that counts and not the perception of the perpetrator of such acts.

1.4 Consequences for Inappropriate Behaviour

Where conduct is found to be unacceptable, the College will implement internal disciplinary procedures. Where conduct is considered illegal, the College will also report the matter to the Police.

Please remember that the UWC Common Code of Conduct and College policies apply to all online activity.

1.5 Digital Communications between Employees and Students (and vice versa)

All digital communications between employees and students (and vice versa) must be professional at all times. Online communication is restricted to the College network and platforms used for Online learning. External platforms not hosted by the College, such as social media sites, ***must never*** be used by members of employees to communicate with students (and vice versa).