Staff and Governors ICT User Agreement

Reviewed:	September 2023
Next Review:	September 2024

This ICT User Agreement forms part of the college's Online Safety Policy. Please familiarise yourself with the Policy before signing this document.

As a professional organisation with responsibility for student's safeguarding, it is important that all staff take all necessary measures to protect data and information systems from abuse, viruses, unauthorised access, damage, loss, and theft. All staff have a responsibility to use the College's computer system in a professional, lawful and ethical manner. This Agreement is designed to ensure that all Staff and Governors are aware of their professional responsibilities when using any form of ICT. All users are expected to sign this Agreement and adhere at all times to its contents. Any concerns should be discussed with the Designated Safeguarding Lead (Andrea Pritchard).

The college has a duty of care towards staff and students, and therefore monitors the use of its ICT systems. This information may be recorded and may be used in disciplinary procedures if necessary, and the college reserves the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request. Use of college ICT systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Loreto is aware that the breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.

Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.

Commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

General

I will only use the college's email/Internet/Intranet and any related technologies for professional purposes or for uses deemed `reasonable' by the Principal or Governing Body.

- I will comply with the ICT system security and not disclose any passwords provided to me by the college or other related authorities.
- I understand that I have a duty to protect my passwords and personal network and Learning Platform logins, and should log off the network / intranet when leaving a workstation unattended or lock it. Any attempts to access, copy, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.

- I will ensure that all electronic communications with students, parents/carers, staff and other professionals are compatible with my professional role. Communication will be transparent and open to scrutiny at all times. It will take place via the college official channels i.e. college email addresses, or telephone number and not via personal devices or other communication channels e.g. personal email, social networking or personal mobile phones. Similarly contact from any of the above to personal email, social networks, personal mobile phones should not be accepted, without specific permission from the Principal.
- I will not give out or make available (electronically or otherwise) my own personal details, such as mobile phone number and personal e-mail address to students or parents/carers, nor will I disclose personal details including phone numbers, fax numbers or personal e-mail addresses of any colleague or student.
- I will not try to access, download, upload or distribute any material that could be considered inappropriate, offensive, illegal, discriminatory, racist, radical or extremist, (such as that referred to in the Prevent Duty Guidance) or may cause distress to others.
- I will not attempt to use any programmes or software that might allow me to bypass the Internet filtering/security systems in place to prevent access to such materials. I will report any accidental access of inappropriate materials to my line manager.
- I will respect and comply with copyright and intellectual property rights.
- I will not use the college ICT systems for personal financial gain, gambling, gaming, political purposes or advertising.
- I will not store or access professional documents which contain college-related sensitive or personal information (including images, files, videos, emails etc) on any personal devices unless they are suitable secured and encrypted. Where possible I will use the college intranet to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft.
- When I use my personal mobile devices in college, I will follow the rules set out in this Agreement and in the BYOD Agreement in the same way as if I was using college equipment.
- I will not engage in any online activity that may compromise my professional responsibilities.
- The College is aware of the huge potential that generative artificial intelligence (GAI) may have on teaching, learning and assessment, as well as wider working practices for both staff and students. Any use of GAI must conform to the values and ethos of the College, as well as being compliant to other College policies including, but not limited to, the GDPR Policy, the Exams Policy and department policies and procedures relating to non-examined assessment (NEA, i.e. coursework), homework and assessment.

Personal Use of Social Media

Please bear in mind that information shared through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation.

The college actively discourages the use of WhatsApp, Chat Rooms, Message Boards or a Facebook Wall for example as a method of raising concerns about matters or grievances that have occurred in college that relate to work colleagues, students etc. Matters of such a nature should be dealt with through the appropriate professional channels.

- I will not invite, accept or engage in communications with parents/carers or students from our college community in any personal social media as in line with College's Social Media Policy.

- I will report any communication received from students on any personal social media sites to the relevant Head of Hall who if necessary will follow the College's Safeguarding Children and Adults Policy and Safeguarding practice.

- I will not communicate with students, in relation to either college or non-college business, via social media, and will only use the college learning platform or other systems approved by the Principal, to communicate electronically with students.

- If I am aware of any inappropriate communications involving any student in any social media I will report it immediately as above.

- I will not accept any current student of any age of the college as a friend, follower, subscriber or similar on any personal social media account.

- I will not engage with any inappropriate social media relationships with ex-students as a friend, follower, subscriber or similar on any personal social media account.

- I understand I am advised to avoid posts or comments that refer to specific, individual matters related to the college and members of its community on any social media accounts. I am further advised to consider the following in relation to social networking sites:
    - Appropriate privacy settings
    - The appropriateness of images and material posted. Once posted online, a message, photo or video clip can be freely viewed, copied, manipulated and circulated and can, potentially, exist forever and ruin professional reputations
    - I will ensure that my online reputation and the use of ICT are compatible with my professional role, whether using college or personal systems. I will take appropriate steps to protect myself online and will ensure that my online activity will not undermine my professional role, interfere with my work duties and will be in accordance the College's Online Safety Policy, Social Media Policy and the Law.

College sanctioned use of Social Media

There are many legitimate uses of social media within the curriculum and to support student learning. For example, the college has an official Twitter account which is managed by the Marketing Manager. Practices for the use of social media for educational purposes can be found in the College Online Safety and Social Media Policies.

Data Protection

- I understand that the college is legally bound by the Data Protection Act and and that the use of personal data must conform to the principles laid out in this Act.

- I will ensure that personal data is kept secure and is used appropriately, whether in college, taken off the College premises or accessed remotely. Personal data can only be taken out of college or accessed remotely when authorised by the Principal or Governing Body. Personal or sensitive data taken off site must be password protected/encrypted.

- I understand that the data protection policy requires that any staff or student data to which I have access will be kept private and confidential, except when it is deemed necessary by law or college policy to disclose such information to the appropriate authority.

- All data held on the college system, including cloud-based repositories, remains the property of the college. Staff do not have an entitlement to copy/download work from any area of the system (including their own user area) when they terminate their employment at the College. Any requests relating to this issue must be made to the Principal.

Email

- I will only use the approved, secure e-mail system for college business.
- When using college email I will use appropriate language. I am aware that as messages can be forwarded or inadvertently sent to the wrong person, email is best regarded as public property and the same professional levels of language and content should be applied as for letters. I will not send anonymous messages or chain emails.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted or if I have any concerns about the validity of the email (due to the risk of the attachments containing viruses or other harmful programmes). I will report such concerns to the Network Manager.

Working with students

- I will support and promote Online Safety with the students and help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- I will support students using video conferencing and will report it to the DSL if it is not being appropriately used i.e. a video link could reveal security details.
- I will ensure that I am familiar with the contents of the Student ICT User Agreement.
- I will not allow students or any other person to use my login and password to gain access to the college ICT system or to use a computer which I have logged onto.
- I will report any student who logs into the college ICT System using another student's login to the relevant Head of Hall.
- I will be alert to the accidental access, by students, to inappropriate materials and report any offending Internet site to the Network Manager.
- I will report all incidents of concern regarding student online safety and any breaches/misuse of the Online Safety policy to the DSL.
- I understand that I am not permitted to use personal digital equipment, such as personal mobile phones and cameras, without permission from the Principal, to record images of students, including when on external trips/visits. With the written consent of parents and staff, the college permits the appropriate taking of images by/of staff and students, using college equipment.
- I understand that images of students and/or staff will only be taken, stored and used for professional purposes in line with college policy and with written consent of the parent/carer or staff member. Images will not be distributed or published outside the college local network without the permission of the parent/carer, member of staff or Principal. Where these images are published eg on the College website intranet it must not be possible to identify by name, or other personal information, those who are featured.
- I will not store images of students on any personal mobile device, neither will I store images of staff without their permission.

- I understand that mobile phones are not to be used to send/receive calls or text messages, in the classroom/teaching situation, unless in an emergency situation.
- I understand that if there are exceptional reasons as to why I am unable to comply with this policy at any time I will immediately outline the exceptional circumstances to the college Safeguarding Officer or SMT for their consideration and advice.