

**E-Safety Policy**

**Introduction**

The City of Liverpool College recognises the benefits and opportunities which new technologies offer to all our students and staff. We encourage the use of technology

not only to enhance students’ learning experience but also to promote skills and achievement. However, the accessible and global nature of the internet and associated technologies means that we are also aware of the potential risks faced and challenges involved.

Our approach is to implement safeguards within the college which will support staff and students to manage any potential risks and to deal with these risks independently. We believe that this can be achieved through a combination of security measures, training, guidance and implementation of our associated policies.

The technologies encompassed within this policy include all computer based technologies, online communication technologies, digital technologies both fixed and mobile.

In addition, we will do all that we can to ensure that all of our students and staff stay

e-safe within our duty of care and within the Every Citizen Matters framework.

This E-Safety Policy should be read in conjunction with other relevant policies, in particular the college Acceptable Use Policy (AUP) for computer equipment, the Social Media Guidelines (Appendix B), the Bullying and Harassment Policy, the Staff Disciplinary and Dismissal Policy and the Student Code of Conduct (Appendix C).

**College E-safety Policy**

The aim of this policy is to develop a co-ordinated approach to e-safety and to promote and safeguard the welfare of all staff and students in a digital world. This will be achieved without hindering students’ e-learning experience, whilst ensuring that skills and knowledge are developed to maximise the use of technology in an appropriate manner.

The policy has been written by the Technology Enhanced Learning Sub Group which is made up of different stakeholders from across the college, including a member of the Senior Management Team, Safeguarding Lead Manager, Quality and Equality Improvement Manager, IT Manager and LRC Manager.

The impact of the policy will be reviewed bi-annually due to the rapid advances in new technologies. The policy will also be considered should there be any concerns raised by the LRC Manager, Safeguarding Team or where an e-safety incident has been recorded or reported.

**Terminology**

Terminology used throughout this document is as follows:

* Site = Facebook or similar.
* Account = login (e.g. personal and/or college/work – you log into your account, using your account login details).
* Profile (Profile Page) = a page that shows personalised information added to your account. E.g. My Personal Facebook profile page is accessed using my personal account details.
* Portal = an Internet portal is a Web site that acts as a starting point for browsing the Web. Portals typically include search engines and large directories of websites. There are also many smaller portals, known as "niche portals," for specific interests.

**Policy Scope**

This policy applies to all students and staff (including agency staff and contractors) of the college community and the use they make of the internet and electronic communication devices such as email, mobile phones, games consoles and social networking sites, whether using college systems or resources of their own. This policy also applies to behaviour towards other people in college using private mobiles.

**Roles and Responsibilities**

There are clear guidelines and lines of responsibility for e-safety within the college.

The first point of contact should be the LRC Manager or a member of the Safeguarding Team. All staff are responsible for ensuring the safety of students and should report any concerns immediately to their line managers (Flow chart Appendix A). Each course team is expected to arrange for students to be made aware of this policy and the ethos of e-safety.

As with the college Safeguarding Policy - staff should take care not to guarantee any measure of confidentiality to any individual reporting any concerns regarding e-safety.

All students must know who to contact if they have any concerns regarding e-safety.

In most cases this will be a member of their course team or the LRC Manager who will also direct any issues regarding e-safety to the appropriate contact:

LRC Manager

The Learning Exchange, Roscoe Street

0151 252 3669

**Security**

The college will do all it can to ensure that the network is safe and secure. Every effort will be made to keep security software up to date and fit for purpose. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, work stations to prevent malicious or accidental access of college systems and information. Digital communications, including emails and internet postings, over the college network, will be monitored in accordance with the Acceptable Use Policy.

Internet usage and monitoring is in place, use of accounts that are password protected enable detailed monitoring to take place, and users also have their own storage and

email accounts that are also subject to monitoring.

**Risk Assessment**

The college is constantly seeking ways to introduce new technologies and will also use Educational Visits as a platform to introduce new systems to students as part of the learning process. In making use of these opportunities, all staff must carry out a risk assessment in accordance with the college Web 2.0 Policy, available to download from the Staff Intranet. All new technologies will be impact assessed to ensure equality of opportunity.

**Behaviour**

Online communication can take many forms, whether via e-mail, text, video conferencing or instant chat/messaging. The college will ensure that all users of technologies adhere to the expected standard of behaviour as set out in the Acceptable Use Policy and/or Staff/Students Code of Conduct -

<http://my.liv-stu.co.uk/information/policies-procedures/acceptable-use-policy/>

The college will not tolerate any abuse of ICT systems or associated technologies. Whether offline or online, communications by staff and students should be courteous and respectful at all times, please refer to the Staff Ethics Policy. Any reported incident or bullying, harassment or other unacceptable behaviour will be treated seriously as set out in the staff disciplinary procedures, the Student Behaviour Policy and Procedure and the Student Code of Conduct (Appendix C).

Where conduct is found to be unacceptable, the college will deal with this internally. Where conduct is considered illegal, the matter will be referred to the Police. Additionally, the college may seek to involve other agencies where conduct is believed to be unacceptable or illegal.

**Communications**

There is a wealth of technologies now available to enhance communication with one another. It is noted that this policy will require continual updating in line with the evolving nature of e-technology and associated communication methods. Electronic communication includes:

* Internet collaboration tools: social networking sites and blogs.
* Internet research: websites, search engines and web browsers.
* Mobile phones and personal digital assistants (PDAs).
* Internet communications: email and instant messaging.
* Webcams and video conferencing.
* Wireless games consoles.

**Data Protection/Personal Information**

Any processing of personal information must be carried out in accordance with the Data Protection Act 1998.

The City of Liverpool College collects and stores the personal information of staff and students regularly e.g. names, dates of birth, email addresses, assessment materials and so on. The college will keep that information safe and secure and will not pass any information onto anyone else without the express permission of the member of staff, student, parent or carer.

No personal information can be posted to the college website without the permission of the person concerned, or their parent or carer.

Staff must keep students’ personal information safe and secure at all times. When using an online platform, all personal information must be password protected and every user is required to log off on completion of any activity.

**Use of Images and Videos**

The use of images, photographs and videos is particularly popular to promote the outstanding work carried out in different curriculum areas, this practice should be encouraged where there is no breach of copyright or the rights of another person.

This includes downloading images from the internet and images belonging to staff and students.

No images, photographs or videos can be copied, downloaded, shared or distributed online without permission from the person. Photographs taken during college activities will be considered carefully and have the consent of the person involved before being published. Unauthorised use of images of the college and/or staff and students will be seen as a breach of the Policy, including images or photographs that have been altered.

**Education and Training**

With the current unlimited nature of internet access, it is impossible for the college to eliminate all risks for staff and students. It is our view, therefore, that the college should support staff and students through training and education. This will provide all users with the necessary skills to be able to identify risks and deal with them independently and manage them effectively.

**Staff (including agency staff and contractors)**

Staff will be offered e-safety training before beginning the new college year, and through staff development sessions throughout the year. This will take the form of E-CPD and will allow tutors hands-on experience, it will also generate further required CPD and following on from the short sessions, guidance and information will be issued to all staff. Any new or temporary users of the college ICT system will be asked to sign the AUP and follow the e-safety rules.

**Students**

Students should have e-safety embedded into all courses using e-learning technologies. Tutorial Advisors and Personal Tutors will be expected to reinforce e-safety messages through the tutorial programme.

When using college PCs, students will be able to see a link to the full policy which includes reporting procedures and how to manage concerns. There will also be posters/leaflets across college and the E-Safety Policy will be included in future Student Handbooks including the flow chart for reporting of incidents. Students should be encouraged to question the viability and reliability of materials researched, viewed or downloaded. They should be encouraged to respect the copyright of other parties and to cite reference properly.

[**http://www.plagiarism.org/**](http://www.plagiarism.org/)

[**http://www.bbc.co.uk/scotland/education/information/copyright.shtml**](http://www.bbc.co.uk/scotland/education/information/copyright.shtml)

[**http://www.vts.intute.ac.uk/detective/**](http://www.vts.intute.ac.uk/detective/)

**Incidents and Reporting**

Where an e-safety matter is reported, the matter will be dealt with very seriously. The college will act immediately to prevent, as far as is reasonably possible, any harm or further harm occurring. If a learner wishes to report an incident, they can do so to their tutor or the college LRC Manager. When a member of staff wishes to report an incident they must inform their line manager, who will inform Human Resources.

Following any reported incident a full investigation will be carried out and the college will decide on the most appropriate course of action. Sanctions may be put in place, external agencies may be contacted or the matter resolved internally depending on the seriousness of the incident. This is in line with the college AUP. Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies.

**Further Information and feedback**

The college welcomes all constructive feedback on this and all college policies. If you would like any further information on e-safety, or wish to send us your comments please contact the LRC Manager.

Useful links for further information:

<http://www.getsafeonline.org>

<http://www.thinkuknow.co.uk/>

<http://cybermentors.org.uk/>

<http://www.digizen.org/>

<http://www.childnet-int.org/blogsafety/yp.html>

**Appendix A**

**Flowchart for responding to e-safety incidents**

E-Safety

Incident

Illegal material or activity found or suspected

Unsuitable materials

Report to IT Manager/HR or Safeguarding Team

Report to LRC Manager/Safeguarding Team

Staff: review incident and decide on appropriate action applying sanctions as necessary (HR involved)

Student: review incident and decide on appropriate action applying sanctions as necessary

IT Manager to secure and preserve evidence

Debrief on e-safety incident

Report to Police, HR and other authorities if appropriate

Review policies and technical tools, and share experience and practice as required

If illegal material or activity is confirmed, allow Police or relevant authority to complete their investigations, seek advice from authorities on treatments of victim and/or offender

If no illegal material or activity is confirmed, revert to internal disciplinary procedures for staff and/or students

Debrief on E-Safety Policy changes

Monitor situation

**Appendix B**

**Social Media Guidelines**

**Introduction:**

Social media portals are powerful communications tools that have a significant impact on organisational and professional reputations. Because they blur the lines between personal voice and institutional voice the following guidelines are designed to help clarify how best to enhance and protect personal and professional reputations when participating in social media.

Social media portals are defined as media designed to be disseminated through social interaction, created using highly accessible and scalable publishing techniques. Examples include but are not limited to LinkedIn, Twitter, Facebook, YouTube, and MySpace. Both in professional and institutional roles, employees need to follow the same behavioural standards online as they would in real life. The same laws, professional expectations, and guidelines for interacting with students, parents, the media etc. apply online as in the real world. Staff are **liable** for anything they post to social media sites.

**Section 1: Guidelines for all Social Media Sites, Including Personal Sites**

Protect confidential and proprietary information: Do not post confidential or proprietary information about the college its students or employees. The Data Protection Act is very specific with regard to the disclosure of personal information without the consent of the owner; any disclosure could result in criminal action against the individual and the college and may result in disciplinary action.

When posting, be mindful of the copyright and intellectual property rights of others and of the college.

Do not use the City of Liverpool College logo on personal social media sites. Do not use the college’s name to promote a product, cause, or political party or candidate.

In accordance with the college’s Acceptable Use Policy you may access personal social media portals only at specified times and locations.

All staff should ensure that personal social networking sites are set at private and that college students are never listed as approved contacts.

Staff should never access social networking sites of students.

There is no longer a distinction between offline and online. If you are going to tweet, post on a Facebook page or contact a student online, it has to be no different to what is appropriate when speaking to them directly.

Obey the Terms of Service of any social media platform employed.

**Section 2: Best Practices**

This section applies to your general use of social media portals in any capacity; it is intended as advice for personal use or as a standard for use associated with the college.

**Think twice:** before posting, privacy does not exist in the world of social media. Consider what could happen if a post becomes widely known and how that may reflect both on the poster and the college. Search engines can turn up posts years after they are created, and comments can be forwarded or copied. If you wouldn't say it at a conference or to a member of the media, consider whether you should post it online.

**Strive for accuracy:** get the facts straight before posting them on social media. Review content for grammatical and spelling errors.

**Be respectful:** understand that content contributed to a social media site could encourage comments or discussion of opposing ideas. Responses should be considered carefully in light of how they would reflect on the poster and/or the college.

**Remember your audience:** be aware that a presence in the social media world is or easily can be made available to the public at large. This includes prospective students, current students, current employers, colleagues, and peers. Consider this before publishing to ensure the post will not alienate, harm, or provoke any of these groups.

**Acknowledge who you are:** On personal sites identify your views as your own. If you identify yourself as a college staff member online, it should be clear that the views expressed are not necessarily those of the college. Consider the use of a disclaimer such as “The postings on this site are my own and do not necessarily represent the position of The City of Liverpool College.”

**Photographs:** posted on social media sites can be appropriated by visitors and altered to convey a different meaning to the original.

**Have a plan**: staff should consider their messages, audiences, and goals, as well as a strategy for keeping information on social media sites up-to-date.

**Link back to the college**: Whenever possible staff posting as part of work-related activity is requested to link back to the college web site. Ideally, work-related posts should be brief; redirecting a visitor to content that resides within the college web environment.

**Protect the college’s reputation**: Posts on social media sites should protect the college’s reputation by remaining professional in tone and in good taste. No individual staff member or faculty should construe its social media site as representing the college as a whole.

**Be aware of liability**: You are legally liable for what you post on your own site and on the sites of others. Individual bloggers have been held liable for commentary deemed to be proprietary, copyrighted, defamatory, libellous or obscene.

**Section 3: Work Related Social Media**

It is recognised that using social media portals as a teaching and learning aid is beneficial; these guidelines are designed to avoid any pitfalls when they are used as part of your working role in the college. Social media should not be seen as negative, there are many sites that can seriously enhance a learning environment and provide an excellent way of communicating with students. The following policies must be adhered to in addition to all the guidelines and best practices listed above:

**Accessing and Using Web 2.0 Services Policy**: Familiarise yourself with the college’s Web 2.0 Policy.

**E-Safety Policy:** Familiarise yourself with the college’s E-Safety Policy.

**Appendix C**

**Code of Conduct**

The college aims to provide a safe and supportive environment where everyone can study and work to the best of their ability. Enrolment onto a course means you have joined the college community and are expected to behave accordingly. You have agreed this by signing the enrolment form.

**We expect you to:**

* Treat other students and staff with respect.
* Be punctual.
* Hand all assignments in on time.
* Achieve the standard of work required of you.
* Let your personal tutor know straight away if you have difficulties with your work.
* Attend all classes and tutorials.
* Notify your local centre office or the relevant course tutor if you will be absent from college. We will assume you have left if you have been absent without explanation for 4 term-time weeks.
* Notify your tutor/assessor if you are absent and cannot keep an appointment with your assessor.
* Keep to the Acceptable Use Policy when using college computers (available under Information on the Student Intranet).
* Follow instructions given by a member of college staff or someone acting for the college (such as a work placement supervisor).
* Give your name and ID to any member of staff who asks for it.

**We will not accept:**

* Unacceptable behaviour in or around college buildings.
* Action which could be seen as harassment of a fellow student or member of staff (for definition of harassment, see the Equality through Quality section in the Student Handbook and Charter).
* Abuse, threats or rudeness to a member of staff. These may be verbal or sent electronically, for example through Facebook.
* The use of illegal drugs or alcohol on or near college buildings.
* Damage deliberately caused to college property or seriously attempted damage to college property.
* Theft, attempted theft or unauthorised possession of any items belonging to the college, or to any students, member of staff or employer.
* Breaking the rules of an awarding body such as copying someone else’s work.
* Repeated problems with the quality of work produced or of handing it in on time, affecting your own and or other students’ chances of gaining accreditation, this may be because of delays in producing work which affects a group project.
* Disruptive behaviour in classes, LRCs or other college spaces or not following a direct instruction from a member of staff.