luminate
EDUCATION GROUP

STUDENT IT AND SOCIAL NETWORKING POLICY – 2020

APPROVED BY (SELT) ON (December 2020)

Applies to:	
Harrogate College	X
Keighley College	X
Leeds City College	x
Leeds Conservatoire	

CHANGE CONTROL

Version:	1.0	
Approved by:	DELT	
Date approved:	December 2020	
Name of author:	Graham Eland	
Name of responsible committee:	DELT	
Related policies: (list)	Student Code of Conduct Relationships at Work Harassment and Bullying (Dignity at Work) PolicySafeguarding Policy Disciplinary Policy and ProcedureData Protection Policy Prevent Duty Guidance- HM Government	
Equality impact assessment completed	**Date:**	
	Assessment type x **Full** ☐ **Part** ☐ **Not required**	
Policy will be communicated via:	College Information Portal andStaff Intranet	
Next review date:	3 years- December 2023	

Contents

1. POLICY AIMS/OBJECTIVES

This policy defines a set of mandatory expectations for students when using computer devices and electronic communications. The primary purpose of thepolicy is to encourage students to achieve standards of use and conduct.

2. Compliance with the IT Policy Framework

It is in all our interests to maintain security over our information and IT assets. You havea responsibility to support this, by protecting the security of your own data/information,and to not access other people's personal systems or information.

You will be held accountable for non-compliance with the mandatory requirements ofthis Policy and Guidance document. Any breaches of the mandatory policy or guidance (where appropriate) will be considered in accordance with the College Disciplinary Policy and Procedure.

To ensure the College staff, students and contractors are aware of their responsibilitiesregarding the use/misuse of IT, this Policy and Guidance document outlines the expectedstandards of use including the following: computer use, illegal or harmful use, email use,social networking and hacking.

3. What is mandatory and what is advisory/guidance?

We have used two headings to describe the relative importance of each section of the document to emphasise what is expected of you and the consequences of non- compliance.

3.1. Mandatory

This is important to us, and you must comply with the policy.

3.2. Advisory/guidance

This is recommended good practice, and should help you in using the computerdevices and electronic communications in the most effective and efficient way.

We use your student number to track system activity in audit trails. This makes allactions performed on College systems attributable to an individual user. Where actions are inappropriate (eg hacking), the ITSS department will be alerted to thisand investigate it together with the Student Life Department and your Student Union.

4. College principles and practices

Our IT systems are for the use of staff and students as part of work and study. You shouldmake use of them for these purposes, and in such a way that will not damage the reputationor the resources of the College.

You are also allowed to use the systems for some non-work/study activities, as long asthese lay within the limits of acceptable use of IT systems and data. Reasonable use includes personal communications (eg emails) and Internet use, as long as these do notdisrupt the work/study of others, threaten the reputation of the College or takes a disproportionate amount of time.

Our systems enable us to monitor telephone call dates/times, e-mail, internet and other communications. For business reasons, and in order to carry out legal obligations in ourrole as an employer, use of our systems including the telephone and computer systems,and any personal use of them, is continually monitored by use of automated software and filtering services. Monitoring is only carried out to the extent permitted or as requiredby law and as necessary and justifiable for business purposes.

The contents of our IT resources and communications systems are our property. Therefore, students should have no expectation of privacy in any message, files, data,document, telephone conversation, social media post conversation or message, or anyother kind of information or communications transmitted to, received or printed from, orstored or recorded on our electronic information and communications systems.

We reserve the right to monitor, intercept and review, without further notice, student activities using our IT resources and communications systems, including but not limitedto social media postings and activities, to ensure that our rules are being complied withand for legitimate business purposes and you consent to such monitoring by your useof such resources and systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings andother uses of the systems as well as keystroke capturing and other network monitoringtechnologies.

If we identify any illegal or concerning activity during monitoring (for example under the Child Protection Act, Radicalisation under the PREVENT Duty or Counter- Terrorism and Security Act) you will be referred as appropriate to the stay safe teamfor support or police for investigation.

The College takes any breach of the Policy very seriously and these will be considered in accordance with the Disciplinary Policy and Procedure. In serious cases, a breach maybe treated as gross misconduct leading to exclusion.

If concerns are raised regarding alleged misuse of Internet access or email content, detailed reports can be provided.

5. Social Networking - how should I use electronic communications (emails, blogs and social media)?

Publication and commentary on social media carries the same obligations as any other kind of publication or commentary. All uses of social media must follow the same standards of conduct that the College students must follow.

The College is committed to the responsible use of the Internet, email and social media.The College may routinely monitor social media and it reserves the right to instruct relevant parties to remove unauthorised sites. Any information posted on social mediasites must comply with the Data Protection Act 2018 and GDPR legislation.

Students must keep a professional distance and not interact with staff online other thanthrough official College social network sites.

Staff are aware of the professional distance and not to interact with students onlineother than through official College social network sites.

All students should be aware that failure to follow the Student IT and Social Networking Policy and any abuse of social media could lead to disciplinary action, and in more seriouscases could be considered gross misconduct and may lead to exclusion through the Disciplinary Policy and Procedure.

5.1. Unacceptable use

5.1.1. Students must not post any material complaining of the College or colleagues on any social media site. Any criticisms of the College or itscommunity members must be made through the College internal procedures.

5.1.2. Students must not say anything contradictory or in conflict with theCollege website.

5.1.3. Students must not post comments that run counter to the CollegesEquality and Diversity Policy and mission.

5.1.4. Students must not post comments that recommend, or appear toendorse actively law-breaking of any kind.

5.1.5. Students must not post comments that exhibit or appear to endorse behaviour that could be argued to encourage “copycat” behaviour by students. This would include for example, dangerous driving, alcohol ordrug abuse.

5.1.6. Students must not participate in using “spyware” software.

5.1.7. Students must not use any of our mail servers or another site's mailserver to relay mail without the permission of the Director of ITSS.

5.1.8. Students must not participate in e-mail bombing, ie flooding someone with numerous or large e-mail messages in an attempt to disrupt them.

5.1.9. Students must not reference any confidential information aboutcustomers, partners or suppliers without their approval.

5.1.10. Do not send inappropriate messages that contravene this policyor related policies listed in this document.

5.1.11. Students must not post any comment that could be viewed as bullying orharassing another student or member of staff. It will be viewed as particularly serious if a student creates a site or page which has the clearpurpose of criticising, bullying or harassing another member. It will also be viewed as particularly serious if a student makes libellous statementsabout any other member or slanderous comments about the College.

5.1.12. Students must not post any comment that explicitly encourages other members of the College community to actively break the law. It will beviewed as particularly serious if a student actively encourages others totake prohibited substances, or commit violence.

5.1.13. Students must not post any comments that promote extremism or radicalisation

6. Computer use - what are my responsibilities?

To ensure clarity of what we (and the law) feel is the appropriate use of our ITsystems, we have set out the boundaries and definitions below.

6.1. Student responsibilities

6.1.1. You have responsibility to protect the security of our systems and data.

6.1.2. You should only access systems and data that are needed for your work orstudies, this includes personal work. IT security controls should prevent youfrom accessing inappropriate systems / information.

6.1.3. You should not share your computer passwords with anyone.

6.1.4. If you have reasonable belief that someone else is abusing the ITsystems, you have a duty to inform your tutor.

7. ITSS responsibilities

Providing support and advice to students, staff and management information whererequired.

JISC is the academic network which links the College with other Colleges/Universities andthe Internet. We all work under the JISC acceptable use policy, and all College studentsare bound by its rules.

8. Student responsibilities – JISC Acceptable Use

8.1. The College and its members may use JISC for the purpose of communicating withother user organisations and its members, and with organisations, individuals andservices attached to networks which are reachable via JISC. All use of JISC issubject to the JISC Terms.

8.2. JISC may be used by the College and its students for any lawful activity. Use by theCollege and its staff and students may be in pursuance of activities for commercialgain as well as for not-for-profit activities.

8.3. It is the responsibility of the College to ensure that its students use JISC services inaccordance with the Acceptable Use Policy and with current legislation.

9. Student responsibilities - JISC Internet unacceptable use

JISC will not be used by the College or its students for any activity that may reasonably beregarded as unlawful or potentially so.

9.1. Unacceptable use (includes but is not limited to these activities)

9.1.1. Creation or transmission, or causing the transmission, of any offensive,obscene or indecent images, data or other material, or any data capableof being resolved into obscene or indecent images or material.

9.1.2. Creation or transmission of material with the intent to cause annoyance,inconvenience or needless anxiety.

9.1.3. Creation or transmission of material with intent to defraud.

9.1.4. Creation or transmission of defamatory material.

9.1.5. Creation or transmission of material such that infringes the copyright ofanother person.

9.1.6. Creation or transmission of unrequested bulk or marketing material tousers of networked facilities or services.

9.1.7. Deliberate unauthorised access to networked facilities or services.

9.1.8. Deliberate or reckless activities having, with reasonable likelihood, any ofthe following characteristics:

9.1.9. Corrupting or destroying other users data

9.1.10. Violating the privacy of other users

9.1.11. Disrupting the work of other users

9.1.12. Denying service to other users

9.1.13. Continuing to use an item of software or hardware after JISC haverequested that use stops because it is causing disruption to the correct functioning of JISC

9.1.14. Other misuses, such as the introduction of “viruses” or other harmfulsoftware.

9.1.15. Creation or transmission of any material linked to terrorism,extremism or radicalisation.

10. What is illegal or harmful use?

You may only access and use the College Internet and network (including email, blogs and social networking) for lawful purposes. You are personally responsible for any transmission you send, post, access, or store via our network, including the content of anycommunication. Examples of illegal or harmful actions that are not permitted

10.1. **Copying/stealing:** copying/stealing of material already written by anotherperson or material protected by copyright, trademark, patent or other intellectual property rights.

10.2. **Offensive materials:** distributing or posting material that is unlawful, defamatory, obscene, indecent, harassing, threatening, harmful, invasiveof privacy or publicity rights, abusive, or inflammatory or otherwise objectionable. You must not access or use our website or network in any manner to send or distribute any images containing pornography.

10.3. **Fraudulent conduct:** offering or distributing fraudulent goods, services,schemes, or promotions (eg make-money-fast schemes, chain letters,and pyramid schemes).

10.4. **Failure to abide by third-party website policies:** violating the rules,regulations, or policies that apply to any third-party network, server, computer database, or website that you access.

10.5. **Harmful content:** distributing or posting harmful content including viruses, Trojan horses, worms, or any other computer programming routines that may damage, interfere with, secretly intercept or seize anysystem, program, data or personal information.

11. What is hacking or disruptive activity?

You must not abuse the security of our website or network in any way.

11.1. Examples of hacking/disruptive activity

11.1.1. **Hacking:** unauthorised access to or use of data, systems or networks,including any attempt to probe, scan or test the vulnerability of a systemor network or to breach IT security without the prior authorisation of theowner of the system or network.

11.1.2. **Interception:** unauthorised monitoring of data or traffic (eg sniffing or keylogging) on any network or system without the prior authorisation of the owner of the system or network.

11.1.3. **Intentional Interference:** interference with service to any user, host ornetwork including, denial-of-service attacks, mail bombing, other flooding techniques, deliberate attempts to overload a system, and broadcast attacks.

11.1.4. **Avoiding System Restrictions:** using manual or electronic means to avoid any limitations established by the College or attempting to gain unauthorised access to, alter, or destroy any information that relates to anythe College or other end-user.

12. Prevent – Due regard to the need to prevent staff From being drawn into terrorism

12.1. There is an important role for the College in helping prevent people being drawn into terrorism. Terrorism which includes not just violent extremism but also non-violent extremism and radicalisation can create an atmosphere conducive to terrorism and can popularise views which terrorists exploit. It is a condition of funding that the College mustcomply with relevant legislation and any statutory responsibilities associated with the delivery of education and safeguarding of learners.

12.1.1. **Further Radicalisation:** Radicalised students can also act as a focal pointfor further radicalisation through personal contact with fellow students andthrough their social media activity. Social Media communications areactively monitored by the College.

12.1.2. **Reporting Attempts to Access Internet Sites:** Effective IT policies and systems are in place which ensure that the signs of radicalisation can be recognised and responded to appropriately. Reports of attempts to accessinternet sites (Radicalisation and Extremism) are notified immediately fromthe Internet Filtering systems to the Head of Safeguarding for review.

12.1.3. **Policies and Governance:** The College has a number of policies includingthis one relating to the use of IT equipment covering what is and is not permissible with Radicalisation and Extremism websites and social networking.

12.1.4. **Internet Filtering:** The College uses Internet Filtering systems for both computers and mobile devices as a means of restricting access to harmfulcontent. Students bringing their own device (BYOD) and connecting to theCollege "Wi-Fi" systems are also protected. The filtering systems are usedas part of the overall strategy to prevent people from being drawn into terrorism, extremism and radicalisation.

12.1.5. **Academic Research:** Access to websites to research terrorism, extremism and radicalisation is blocked by default. A request to access internet sites of this nature must be requested through the ITSS Service Desk who will forward the request and liaise with the Head of Safeguarding.

13. APPENDIX 1

HOW TO USE SOCIAL MEDIA – GUIDELINES FOR STUDENTS

Background

Social media provides wonderful opportunities for life and for learning. The term social media describes the online tools, websites and services that people use to share content, profiles, opinions, insights, experiences, perspectives and media itself. These tools include social networks, blogs, message boards, podcasts, microblogs, lifestreams, social bookmarking, wikis and vlogs. The feature that all these tools, websites and services have in common is thatthey allow conversations and online interactions between groups of people. These guidelinesare not intended to deter individuals from using these communication tools but are necessaryto help protect staff and students and to prevent them damaging the college either inadvertently or intentionally.

All students should be aware that failure to follow these guidelines could lead to disciplinaryaction, and in more serious cases could be considered gross misconduct and may lead to exclusion.

The College is committed to the responsible use of social media. The College may routinely monitor social media and it reserves the right to instruct relevant parties to remove unauthorised sites. Any information posted on social media sites must comply with the DataProtection Act 2018 and GDPR legislation.

Related Policies and documents

These documents should be read with reference to the following the College policies and documents and are available on the student intranet:

- Positive Behaviour and Disciplinary Policy and Procedures

- Policy against Harassment and Bullying
- ITSS Policies and Procedures
- Code of Conduct
- Safeguarding Policy
- Data Protection Policy
- Equality and Diversity Policy.

The widespread use of social media such as Facebook, You Tube, Instagram and Twitter raises issues for the College in terms of interactions between students and between studentsand staff. Students and staff may be unaware of the implications of their comments/postings.Internet interactions between staff and students have the potential to be much less professional than they would in other contexts.

These policies have been developed to:

- Give staff and students the tools to use social media responsibly
- Make clear to staff and students the limits of “free speech” on theInternet Draw clear boundaries that it would be inappropriate to cross
- Lay out the potential penalties for breaking the guidelines or the attendant policies.

Mindfulness around all aspects of internet communication is recommended as it must be remembered that that all communication on the Internet must be considered as in the public domain and can be difficult to remove.

Social media in relation to students

Students need to understand that as members of a wider college community they do not havetotal freedom to express themselves as they wish. The following types of communication arenot allowed and will result in the Positive Behaviour and Student Disciplinary Policy being used.

Students are reminded that material posted on the Internet can be very hard to remove. Students are advised not to post photographs of themselves or other members of the community that they might not wish others to see now or in the future. They would also bewell-advised not to make written comments that could be used against them in future.

14. GUIDANCE NOTES

Protect your own privacy

Privacy settings on social media platforms that might allow others to post information or see information that is personal should be set to limit access. Be mindful of posting information that you would not want the public to see.

Be Honest

Do not blog anonymously, using pseudonyms or false screen names. Do not say anything that is dishonest, untrue, or misleading. What you publish will be around for a long time, soconsider the content carefully and be cautious about disclosing personal details.

Respect copyright laws

It is critical that you show proper respect for the laws governing copyright and fair use or fair dealing of copyrighted material owned by others; including the College own copyrights and brands. You should never quote more than short excerpts of someone else's work, and always attribute such work to the original author/source. It is good general practice to link to others' work rather than reproduce it. The College has plagiarism software which will detect work completed by others.

Respect your audience

The public in general, and the College's employees, customers and students, reflect a diverse set of customs, values and points of view. Don't say anything contradictory or in conflict with the College website. Don't be afraid to be yourself, but do so respectfully. This includes no offensive comments, defamatory comments, personal insults or obscenity) but also proper consideration of privacy and of topics that may be considered objectionable or inflammatory - such as politics and religion. Use your best judgment and be sure to make it clear that the views and opinions expressed are yours alone and do not represent the official views of the College.

Be the first to respond to your own mistakes

If you make an error, be open about your mistake and correct it quickly and visibly. If you choose to modify an earlier post, make it clear that you have done so. If someone accusesyou of posting something improper (such as their copyrighted material or a defamatory comment about them), deal with it quickly.

Social Media Tips

The following tips are not mandatory, but will contribute to successful use of social media:

- Set your comments setting, when possible, so that you can review and approve thembefore they appear.
- Remember: employers are increasingly conducting web searches on job candidates before extending offers. Be sure that what you post today will not come back to hauntyou.
- While you want to be honest about yourself, don’t provide personal information that couldbe used against you.