IT SERVICES POLICIES AND PROCEDURES	LEWISHAM SOUTHWARK COLLEGE
Policy title:	**IT Systems and Social Networking policy and procedure**
Applies to:	**All employees/visitors/agency workers/contractors/students**
Owner of Policy:	**IT Services (ITS) Department**

1. Introduction and scope

1.1 The ability of people to use computers, e-mail and access the Internet provides new opportunities for the College as it facilitates the gathering of information and communication between employees, students, customers and others. However, the use of computers, the Internet and e-mail exposes the College to new risks and liabilities. It is therefore essential that everyone reads this policy and becomes aware of the potential risks involved in using computers, e-mail and the Internet.

1.2 This policy applies to all employees, visitors, agency workers, contractors and students using computers connected to the College network.

2. Policy objectives

2.1 This policy aims to:

- Provide a framework for the appropriate use of computers, the internet and email within the College;
- Provide IT users with clear guidelines on the unacceptable use of IT facilities.

3. Responsibilities: Managers

3.1 Managers are required to:

- Ensure that they and their employees are aware of the policy and when its use may be appropriate;
- Investigate unauthorised or inappropriate use of IT systems and to liaise with the IT and HR Department as appropriate;
- Apply and operate the policy fairly and consistently.

4. Responsibilities: Employees/Visitors/Agency Workers/Contractors/Students

4.1 Employees, visitors, agency workers, contractors and students are required to:

- Familiarise themselves with this policy;
- Comply with the provisions of this policy.

5. General points

5.1 Use of computers, telephones, e-mail and the Internet are primarily for work-related or study purposes. Limited personal use is allowed, but should be restricted to breaks and before and after normal working hours.

5.2 The College has the right to monitor, and will monitor, all aspects of its telephone and computer systems that are made available and intercept or record any communications, including telephone, e-mail or Internet communications. Remote viewing software to monitor desktop screens can also be used by new technologies. Monitoring is carried out to:

- Ensure that College facilities are being properly used for the conduct of its business including teaching and learning;
- Ascertain compliance with legal requirements and provisions of this policy;
- Investigate or detect unauthorised or inappropriate use of telecommunications or IT.

5.3 The College reserves the right to use the content of any e-mail, websites visited or files held on the College network in any disciplinary process.

5.4 All College email accounts are the property of the College.

5.5 It is inappropriate for users of the College Internet system to access or attempt to access, download or transmit any material which might reasonably be considered to be obscene, abusive, sexist, racist, defamatory, discriminatory (as defined in the Equality Act 2010), related to violent extremism or terrorism or which is intended to annoy, harass or intimidate another person in any way.

5.6 Employees should be aware that this also applies to use of social media systems accessed from both College systems and personal devices and that such material may be contained in jokes, spam, on line banter, on Twitter, text messages and or social networking sites such as Facebook, etc.

5.7 Cyber bullying or harassment through any means is a disciplinary offence and in such instances the College's student or employee Disciplinary policy and procedure will be invoked.

5.8 Any breach or suspected breach of this policy should be reported to the Data Protection Officers of the College. The Data Protection Officer concerned will review the case and decide whether the matter should be investigated and by whom.

5.9 Breaches or suspected breaches of this policy involving extremism will be shared with the Designated Safeguarding Officer.

6. Authorisation to use College IT facilities

Employee log ins are for employee use only. Password(s) must be kept secure and should not be disclosed to or used by anyone else. For reasons of security, passwords should not be printed or stored online. Employees are not permitted to log in for other users using their account log in details.

7. Inappropriate use of College IT facilities

7.1 Employees are not permitted to use the College computing, email or Internet facilities for any of the following:

- Participation in distributed file sharing;
- Making voice calls over the Internet for personal use;
- Using Internet chats or messenger software for personal use;

- Providing commercial services through web pages supported on the College network, or the provision of 'home-page' facilities for any commercial organisation;
- Unlawful activity including copying and removing confidential data files or copyright restricted programs from the College computers or networks on any removable storage media;
- Creating or transmitting defamatory material about any individual or organisation;
- Sending any communication that does not correctly identify the sender or attempts to disguise the identity of the computer from which it was sent;
- Creating, transmitting or accessing material in such a way as to infringe a copyright, moral right, trade mark, or other intellectual property right;
- Using College Internet and email facilities for private profit;
- Gaining or attempting to gain unauthorised access to any facility or service within or outside the College, or making any attempt to disrupt or impair such a service;
- Activities not directly connected with employment, study, or research in the College (excluding reasonable and limited use of social media for recreational purposes where not in breach of these regulations or otherwise forbidden) without proper authorisation;
- Plagiarism – (passing off someone else’s work as ones’ own) whether intentionally or unintentionally;
- Sending emails or registering on third party websites which could enter the College into legally binding contracts or obligations – unless the user has express authority to do so or has obtained appropriate permissions;
- Misleading someone about their true identity or using someone else’s computer accounts;
- Online betting, gambling or pornography;
- Online shopping, including buying and selling on eBay.

8. Connection of computers to the College networks

8.1 Users who bring computers or other devices which are capable of connecting to the wired or wireless College networks must ensure compliance with College standards for secured connections to the network.

8.2 No computer or other device connected to the College networks directly or indirectly may be used to give any unauthorised person or computer system access to any restricted resources within the College.

9. Copyright and downloading

9.1 Copyright applies to all text, pictures, video and audio. In general employees may download and use such files but may not forward them on to others without the permission of the author of the material or an acknowledgement of the original source of the material, as appropriate.

9.2 Any files downloaded to the College network should be of a reasonable size depending on work or study requirements.

9.3 Users must not download files whose source or authenticity cannot be verified using the College’s computer network.

9.4 Any suspect emails must not be opened and should be reported to the IT Services Department.

10. Data protection

10.1 Users of IT systems wishing to hold or process data relating to a living individual should do so in accordance with the provisions of the College's Data Protection policy and procedure. Advice can be sought from the HR or IT Services Departments.

10.2 Any data protection rules or regulations applicable to electronic media such as computer files, databases or emails are also applicable to their printed copies.

10.3 Users must ensure that information printed, downloaded, copied or transferred is handled and stored (for example on USB drives) with care and confidential printouts are destroyed when no longer needed according to the prescribed College procedures on managing confidential data.

11. E-mail and Internet usage

11.1 Reasonable private use of email or the Internet is permitted in line with College procedures for staff and students but should be kept to a minimum. Excessive personal access to the Internet during working hours may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct.

11.2 E-mails should be drafted with care as they are legal documents and can be used in disciplinary/grievance processes or as evidence in court.

11.3 Users should not make political or derogatory remarks in e-mails or on social networking sites about the College, employees, students, competitors or any other person. Any such remark may constitute libel or breach other legislation. It could also lead to disciplinary action.

11.4 By sending e-mails on the College's system, employees are consenting to the processing of any personal data contained in that e-mail and are explicitly consenting to the processing of any sensitive personal data contained in that e-mail. If employees do not wish the College to process such data they should communicate it by other means.

11.5 Websites accessed by employees must comply with the restrictions set out in this policy. Accessing or attempting to access inappropriate sites may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct under the employee or student disciplinary policies.

11. 6 All access or attempted access to the Internet is recorded on the College Internet filtering software. These records will be inspected if misuse is suspected.

12. Social networking websites, personal web pages and web blogs

12.1 Although the College respects computer users' right to personal and social interaction, it must also ensure that information security and reputation are protected. The College therefore requires all users to:

- Ensure that they do not conduct themselves in a way that is detrimental to the reputation or interferes with the business interest of the College;
- Ensure that no information is made available that could provide a person with unauthorised access to the College systems and/or any confidential information;
- Refrain from recording any confidential information regarding the College on any social networking websites;
- Take care not to allow their interactions on these websites to damage working relationships between employees, and students or between students;
- Ensure personal blogs and web pages on social networking sites are not used to attack or abuse anyone;
- Ensure they respect the privacy and feelings of others;
- Not use personal accounts on social networking sites for College business (including interactions with students).

12.2 Accounts dedicated to teaching and learning can be established with agreement from the Head of Department or line manager.

12.3 Any blog, etc. in which the College is mentioned as an employee's place of work or study should also contain a disclaimer that the views expressed in the blog are the employees' alone and do not represent the views of the College.

12.4 Any employee wanting to start a blog where they are identifying themselves as a College employee should speak to their manager. IT services will be able to answer questions on what is appropriate to include in a blog.

12.5 It should always be clear to users whether the site they are interacting with is a College page run by the College for College purposes or whether this is a personal page run by an individual for their own private purposes.

12.6 At no stage during the recruitment or enrolment process should recruiting managers, HR staff or tutors conduct searches on prospective employees or students on social networking websites.

12.7 Creating or endorsing "hybrid" sites which contain elements of both should be avoided as this is likely to cause confusion, editorial problems and brand damage. For example, a tutor's personal profile should not have a URL which contains a College brand or programme/project name.

13. Exceptional access requirements

13.1 Any exceptional access requirements on the computer systems or networks which are not covered by this policy but are needed for the conduct of College business must be authorised by the Head of IT Services.

14. Reporting of achievement of/compliance with the policy

14.1 This policy will be reviewed and amended in line with changes to legislation and/or College procedures. Where relevant, compliance will be monitored by the HR Department. Comments or suggestions about this policy should be referred to the HR Department in the first instance.

15. Linked policies and procedures

15.1 This policy is linked to the following policies:

- Data Protection policy and procedure;
- Bullying and Harassment policy and procedure;
- Disciplinary policy and procedure.

16. Impact assessment

16.1 This policy was equality impact assessed in: May 2016.

Approved by:	Executive - April 2016
Publication date:	April 2016
Review date:	October 2018