IT AND SOCIAL MEDIA ACCEPTABLE USE POLICY

POLICY STATEMENT:

EKC Group provides information technology (IT) to enable staff and students to fulfil their work and academic commitments and responsibilities and to enhance teaching, learning and assessment. If IT is deliberately or unintentionally misused, the safety and security of data, business continuity and potentially the reputation of the college may be adversely affected. The manner in which staff and students conduct themselves in the use of IT is therefore of key importance and all users must ensure that they are compliant with this policy. The EKC Group will undertake to make users aware of the policy at staff and student inductions and other appropriate opportunities.

The policy relates to all authorised users of the EKC Group's IT network and services and covers the following key areas:

- General responsibilities of authorised users
- Emails
- Use of the internet
- Use of social media
- Software, copyright and downloading
- Use of telephony
- Cloud computing
- Consequences of violation

PROCEDURES:

General responsibilities of authorised users

An authorised user (staff, student, Governor, authorised consultants and volunteers) of the college's IT systems will have a user account issued to them in accordance with college IT security procedures. In accepting and using their account, users agree to the following general conditions as well as the specific procedures as detailed in this document:

1. All individually allocated user accounts, passwords and email addresses are for the exclusive use of the individual to whom they are allocated. Users must 'lock' their laptops/PCs when they are away from their workspaces to prevent other users from accessing their accounts. Users are personally responsible and accountable for all activities carried out under their user account. The password associated with a particular user account must not be divulged to any other person, other than to designated members of IT staff for the purposes of system support.
2. Attempts to access or use any user account or email address which is not authorised to the user, are prohibited.
3. Users must take all reasonable precautions to protect their passwords. Individual passwords should not be printed, stored on-line or given to others.
4. Users must not deliberately introduce any virus or other harmful programme to the college's IT systems

5. Users agree to treat IT hardware and equipment with respect and to avoid damage or loss as far as possible.
6. Users must alert the the Group's Data Protection Officer at the earliest possible opportunity in cases of theft of, or damage to, hardware and/or the possibility of any breach to the integrity of IT hardware, software or user accounts.
7. Use of IT systems and hardware must not contravene legislation and must not harm others.
8. Users must not introduce new IT software or hardware without consultation with and permission from the Group's Leadership Team. In all cases, the risks of processing data on new software or hardware must be assessed by carrying out a Data Protection Impact Assessment.
9. No personal or sensitive information on Learners, Applicants, Employees or Employers (as covered by Data Protection legislation) should be copied or stored on personal storage or personal devices including USB and personal cloud storage.) IT staff can provide guidance on how to encrypt and store and send data securely if normal methods are not usable.
10. The college does not routinely monitor email other than automated scanning for viruses, 'spam' and access to unauthorised internet sites. However the college reserves the right to intercept email and internet communications within the terms of the Regulation of Investigatory Powers Act (2000) and to take action as appropriate.
11. The EKC Group routinely monitors all users' internet use. A daily report is reviewed by the senior staff at each College and the Senior Designated Safeguarding Officer. Any inappropriate use will be discussed with the user and escalated where necessary to a Prevent Officer or Designated Safeguarding Lead as appropriate.
12. If users have any suspicions about any files or email communications e.g. virus or hoaxes, they should not open the file but must immediately contact the IT helpdesk so that the matter can be investigated.
13.

Authorised staff, Governors, consultants or volunteer users must adhere to the requirements and principles of safeguarding when using IT and telephony to communicate with students. This means not engaging in activity that could compromise professional relations or bring safeguarding into question. For example, staff must not: Divulge personal details such as email addresses and telephone numbers to students or
communicate on a personal level via social media. Staff are asked to set up a WAMedu group to communicate with current students. Facebook, Twitter etc can be used for promotional purposes via official college channels and must adhere to the Social Media Best Practice Guidelines. (Twitter, Facebook, MySpace etc)

14. Staff must not use personal devices or channels to communicate with students or store information about students e.g. photographs, student data etc.
15. When a member of staff leaves the EKC Group's employment, any current employment references to EKC Group on social media, such as LinkedIn must be removed within 48hrs.
16. If a curriculum area or service area wishes to set up a social media account such as Facebook or Twitter, permission must be sought from Marketing. Curriculum staff must exercise professional judgement when posting content to internal or external EKC social media. Content must not be of a nature that will potentially bring the college into disrepute or be offensive to the viewer. Guidance on what can be posted on these accounts is available from Marketing and must adhere to the Social Media Best Practice Guidelines.

Useful information about the safe and secure use of IT and social networking can be found on the Get Safe Online website.

Email use

General principles

17. The EKC Group's email system (including instant messaging) is provided for work and academic purposes. Email accounts and the data stored in them are the property of the EKC Group; whilst the college will take all reasonable steps to respect the privacy of email communications, users should have no expectation of privacy in any email sent or received, whether it is of a business or personal nature. Where the content of emails is to be accessed for any of the purposes detailed below, the action must be approved by a member of the Group's Leadership Team following due process. Instances where the college may have to interrogate emails are as follows.

- Unexpected or prolonged absence of a member of the college where not dealing with his or her email in a timely manner adversely affects business operations.
- To fulfil a legal requirement e.g. a Subject Access Request under Data Protection legislation
- To assist in disciplinary investigations.
- To investigate possible criminal activity.

18. Email is recognised as a formal method of communication and has the same status in law as the printed word. Users could incur legal liability for themselves and/or the college on the basis of information provided or opinions expressed by email. The tone and content of emails should therefore be appropriate, accurate and professional at all times.

19. Staff should not create email congestion by sending trivial messages or unnecessarily copying emails. Unnecessary emails should be deleted regularly to prevent over-burdening the system. Files should also be deleted from deleted and sent items.

20. Staff should be aware that the email system is not designed as an efficient system for the long-term storage/archive of important information. Emails which need to be retained for record keeping purposes, should be saved in text/html format within the relevant working directory structure. Student emails are not archived.

21. Reasonable personal use of email by staff is permitted but should not interfere with work obligations and should be outside of normal working hours. The contents of personal emails must comply with the restriction set out in this policy document. Regular use of the email system for non-business purposes during working hours may lead to disciplinary action and may in certain circumstances be treated by the EKC Group as gross misconduct.

22. By sending emails on the EKC Group's system, users are consenting to the processing of any personal data contained in that email and are explicitly consenting to the processing of any sensitive personal data contained in that email.

23. Emails sent outside the college should include the college standard signature and a notice which will automatically be appended to the following statement: :

    "This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you are not the intended recipient or the person responsible for delivering the email to the intended recipient, be advised that you have received this email in error and that any use, dissemination, forwarding, printing, or copying of this email is strictly prohibited."

    Note – Student email accounts have a slightly different disclaimer stating that any views/comments expressed are those of the sender and NOT the EKC Group.

24. To ensure compliance with theFreedom of Information Act and Data Protection legislation, and to maintain the high service standards of the EKC Group, staff who are away from the office must make arrangements to ensure that their emails are properly dealt with either by using the remote access facility, or configuring an out of office message giving the email address of a colleague dealing with issues arising in their absence.

25. Staff who are on long term absence e.g. sickness, maternity, paternity, compassionate leave etc. should access their emails only if they wish to, for example, to keep up to date. HR will liaise with the member of staff to determine their wishes in this respect. When the member of staff returns to work, their manager should seek to update them on a face to face basis rather than by email to assist their integration back into the working environment.

26. Staff should be mindful of when emails are sent. The college places no expectation on staff to send or respond to emails during holidays, weekends or whilst on leave of absence for whatever reason.

27. Emails should not be used in favour of face to face or telephone communication.

28. Emails to 'all staff' that relate to cross-college matters must be approved by the Group Principal; if approved for circulation they will be posted by the Senior Executive Officer. Emails to 'all staff' that relate to individual College matters must be approved by the relevant College Principal.

29. The maximum size of attachment that can be sent is 5MB. Where large files need to be transmitted they should be put into a zip file.

30. Emails that are flagged as private or confidential should not be forwarded or shared without the permission of the originator.

<u>Unacceptable use of the email system</u>

31. Creation or transmission of material which brings the college into disrepute.
32. Creation or transmission of material that is illegal.
33. The transmission of unsolicited commercial or advertising material, chain letters, press releases or other junk-mail of any kind.

34. The unauthorised transmission to a third party of confidential material concerning the activities of the college.
35. The transmission of material that infringes the copyright of another person, including intellectual property rights.
36. Activities that unreasonably waste staff effort or networked resources, or activities that unreasonably serve to deny service to other users.
37. Activities that corrupt or destroy other users' data or disrupt the work of other users.
38. Creation or transmission of any offensive, obscene or indecent images, data or other material.
39. Creation or transmission of material that is libellous, abusive or threatening to others, serves to harass or bully others, discriminates or encourages discrimination on the basis of ethnicity, gender, sexual orientation, marital status, disability, age, political or religious belief. This includes any material that has, or could be considered to have, the potential to radicalise or incite racial or religious hatred.
40. Activities that violate the privacy of others or unfairly criticise, misrepresent others; this includes copying distribution to other individuals.
41. Creation or transmission of anonymous messages or deliberately forging messages or email header information, (i.e. without clear identification of the sender.)
42. The unauthorised provision of access to the EKC Group's services and facilities by third parties.

Internet use

General principles

43. Users are expected to use the internet access in a responsible, efficient, ethical and legal manner. Internet access is a privilege, not a right, and access will be revoked for anyone who violates the conditions of this policy.

44. Reasonable private use of the internet by staff is permitted but should be kept to a minimum and should not interfere with work. Excessive private access to the internet during working hours may lead to disciplinary action and may in certain circumstances be treated by the EKC Group as gross misconduct.

Unacceptable use of the internet

45. Creation, transmission or distribution of offensive, obscene or indecent images, speech or material.
46. Creation, transmission or downloading and distributing material which infringes copyright regulations.
47. Transmission of commercial or advertising material, or political lobbying.
48. Activities which waste staff time or networked resources, including participation in "Chat Rooms".
49. Destruction of other people's data.
50. Wilful downloading or uploading of any form of computer virus.
51. Downloading, storing or distributing material which would be considered inappropriate, offensive or disrespectful to others, or advocates or condones the commission of unlawful acts,

violence or discrimination against other people. This includes materials that have, or could be considered to have, radicalisation objectives. N.B. the internet is monitored continually and any individuals accessing such materials will be dealt with via appropriate EKC Group policies and procedures. Where appropriate, the Police and Counter Terrorism services may be engaged to assist in an investigation.

52. Sending chain letters via email.
53. Downloading email attachments from people you don't know - these may contain viruses.
54. "Spamming" - distributing mass unsolicited messages to email addresses or Newsgroups.
55. Financial gain or advertising.
56. Pirating of illegal software/files.
57. Impersonation, anonymity or pseudonyms - any communication on the internet via email or otherwise is the responsibility of the person who issues it.

Social media

58. Social media/networking (Facebook, LinkedIn, Twitter, blogs, wikis etc.) can be a valuable tool in communicating the EKC Group's offer to the wider world and in adding value to the curriculum and student experience; however these media may be subject to unwitting abuse by users and it should be noted that the college can be held vicariously liable for any inappropriate or illegal use of social media. To ensure, as far as possible, that users are aware of their responsibilities with regard to social media, the college will undertake to regularly brief all users of IT on e-Safety and acceptable use of social media.

The following key principles with regard to social media should be observed at all times:

59. Communications must not include anything that could be considered libellous, illegal, offensive, defamatory or that may bring the EKC Group into disrepute/adversely affect the college's reputation.
60. The EKC Group takes bullying and harassment extremely seriously. Members of staff or students who use social media to bully and harass will be subject to the relevant disciplinary procedures.

61. The broadcasting of personal data/information without a person's knowledge is prohibited

62. Staff are not permitted to communicate with students via social media apart from through authorised social media channels e.g. the EKC Group Facebook site. Any communication with students via authorised social media should relate to college business only.

63. Marketing will authorise, establish and support EKC Group social media sites. Any existing social media accounts that engage students in non-promotional activities (e.g. study Programme groups) should be closed with students and staff engaging on WAMedu.

64. Personal views should be qualified by the individual making the statement; it should be made clear that the views are personal and do not reflect the views of the college.

65. Staff should not engage in communications about potentially sensitive or political topics or legal matters relating to the college.

66. Any communication via social media must always by respectful and accurate and avoid the possibility of incorrect assumptions being made.

Software, copyright and downloading

67. Copyright applies to all text, pictures, video and sound, including any media sent by email or the internet. Files containing copyright protected material may be downloaded but not forwarded or transmitted to third parties without the permission of the originator or an acknowledgement of the source of the material.

    Software available on the college network may only be used subject to the relevant licencing agreements for that particular piece of software. Software must never be downloaded copied or installed without the express permission of the Head of Technology
68. Users should not import non-text files or unknown messages onto the college's system without having them scanned for viruses.

69. The downloading of executable files from the internet or via email is prohibited. These files can often introduce viruses which can damage the IT network. If you are unsure, please contact the IT helpdesk.

Use of Telephony

Telephony (mobile telephones, handsets, headsets etc) is provided for business purposes. Staff may use telephony (or texts in the case of mobile telephones) for essential or emergency matters but must reimburse the EKC Group for the cost of the call(s)/text(s).

Cloud Computing

Use of cloud based applications (e.g. Googledocs, OneDrive, DropBox etc) must be risk assessed to ensure that they do not contravene Data Protection legislation: cloud providers are likely to store and move data around multiple servers situated in a number of jurisdictions which are likely be outside the European Economic Area (EEA). This can result in a breach of the Data Protection legislation unless there are adequate security measures in place for personal data. Compliance may be achieved if EU approved contract terms are used with a cloud provider. Under no circumstances must personal or sensitive data as defined in Data Protection legislation be stored in cloud based applications.

When conducting a risk assessment for cloud computing the following aspects should be covered:

- What "Information Security Standards" does the provider adhere to?
- Does the cloud provider use third parties to evaluate its own security risks?
- What identity and access management architecture is in place?

- How will the cloud provider accommodate the obligations that the institution has with regard to data protection and data retention schedules?
- Are there clear penalties in the contract for data loss or breach of security and privacy?
- Can the cloud provider give assurances that information can be taken down without delay from websites or other accessible locations on the instruction of IT services?
- What planned responses are in place should a service failure occur?
- Can the cloud provider's facilities be inspected by the institution's IT services?
- Is data portability part of the service that is provided?
- Where encryption of data is required is the cloud provider able to facilitate this requirement?

The risk assessment should be referred to the the Group's Data Protection Officer) before any cloud based sites are established. Further useful information on cloud computing can be found on the UK Data Service website http://ukdataservice.ac.uk/manage-data/store/file-sharing.aspx

Consequences of violation

Where users are found to violate any aspect of this policy, they will be subject to the immediate withdrawal of user rights and the instigation of disciplinary procedures. Individuals may also be subject to criminal proceedings. The EKC Group reserves its right to take legal action against individuals who cause it to be involved in legal proceedings as a result of their violation of licensing agreements and/or other contraventions of this policy.

Students are referred to appendix 1 of this policy for a user friendly guide to the above Policy.

Relevant policies and procedures

Data Protection Policy
Remote, Mobile and Homeworking Procedure
Safeguarding and Preventing Extremism and Radicalisation Policy
Conduct of Staff Policy