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 and financial standing of the Group may be adversely affected. Personal data could also be compromised which could lead to a data security breach and investigation and prosecution by the Information Commissioner's Office.

Cybercrime represents a real and immediate threat and can cause significant and far reaching damage to an organisation. If all staff and students use the Group's IT systems correctly and appropriately, the risk of the Group's systems being hacked or held to ransom is reduced.

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. EKC Group will undertake to make users aware of the policy at staff and student inductions and other appropriate opportunities. In addition, staff are required to complete mandatory training on cyber security and Data Protection.

This policy applies to everyone who is allowed to use EKC Group's IT network and services. It is divided into sections based on who you are:

- **Visitors and Guests**: Read Part A.
- **Students**: Read Parts A and B.
- **Staff**: Read Parts A, B, and C.

The policy covers these important areas:

1. General responsibilities of users
2. Email usage
3. Internet usage
4. Social media usage
5. Software, copyright, and downloading
6. Telephone usage
7. Cloud computing
8. Using Teams and online working/learning
9. Consequences of breaking the rules

Part A – All Users including guests and visitors

1. Any deliberate hacking/testing without prior authorisation by Group Director of Digital will be referred to the most appropriate disciplinary stage in accordance with relevant policy/procedure.
2. Attempts to access or use any user account or email address which is not authorised to the user, are prohibited.
3. Users must not deliberately introduce any virus or other harmful programme to the Group's IT systems and must advise IT immediately of any actual or suspected threats to the integrity of the network and data.
4. Users agree to treat IT hardware and equipment with respect and to avoid damage or loss as far as possible.
5. Use of IT systems and hardware must not contravene legislation and must not harm others.
6. Activities that violate the privacy of others or unfairly criticise, misrepresent others; this includes copying distribution to other individuals.
7. Creation or transmission of anonymous messages or deliberately forging messages or email header information, (i.e. without clear identification of the sender.)
8. The unauthorised provision of access to EKC Group's services and facilities by third parties.
9. 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.
10. AI tools must not be used to process, share, or generate content involving identifiable personal data - including but not limited to photos - without explicit authorisation and adherence to data protection policies. Misuse may result in disciplinary action.

Relevant policies and procedures for guests and visitors

- Data Protection Policy
- Safeguarding and Preventing Extremism and Radicalisation Policy
- Online Safety Procedure

Part B – Students

In addition to the terms in Part A, students must also follow these guidelines:

An authorised user (staff, student, Governor, authorised consultants and volunteers) of the Group's IT systems will have a user account issued to them in accordance with Group 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.
2. 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.
3. Users must use 'strong' passwords in accordance with the protocols advised in cyber security training.
4. Users must take all reasonable precautions to protect their passwords. Individual passwords should not be printed, stored on-line or given to others.
5. Users must alert the Group's Data Protection Officer on dpo@eastkent.ac.uk within 24 hours in cases of theft of, or damage to, hardware and/or the possibility of any breach to the integrity of personal data, IT hardware, software or user accounts.
6. The Group does not routinely monitor IT usage, except for automated scanning for viruses and spam. However, the Group reserves the right to review and investigate all activities on its IT resources, including email, internet usage, Teams/OneDrive, and social media. We may search, monitor, and read all communications sent or received on EKC Group computers and take action if inappropriate use is suspected or in cases of a personal data breach. Such searches and monitoring may also be conducted to gather evidence for conduct, disciplinary, or whistleblowing matters.
7. Searches may be carried out under the Regulation of Investigatory Powers Act (2000) and the results may be shared with law enforcement agencies. All searches will have a justifiable reason and be authorised by the College/Business Unit's Principal/Director. No notice will be given of such searches.
8. EKC Group routinely logs all users' internet use and access to unauthorised internet sites. A daily report is reviewed by the senior staff at each College and the Senior Designated Safeguarding Officer and internet usage reports may also be interrogated by an Investigating Officer in the event of inappropriate use. Any inappropriate use will be discussed with the user (where it is appropriate to do so) and escalated where necessary to a Designated Safeguarding Officer or Designated Safeguarding Lead in the case of students or to a senior Manager in the case of staff. Where there has been inappropriate use of the internet by staff or students, this may result in disciplinary proceedings. Monitoring may be carried out under the terms of the Regulation of Investigatory

Powers Act (2000), the results of which may be shared with law enforcement agencies where necessary.

9. Emails that are flagged as private or confidential should not be forwarded or shared without the permission of the originator. Exceptions to this may be applied where a person's welfare is compromised or there are significant matters which need to be brought to the attention of senior leadership for investigation.

10. <u>What is classed as unacceptable use of the email system</u>

- Using someone else's email address to send messages.
- Creation or transmission of material which brings the Group into disrepute.
- Creation or transmission of material that is illegal.
- The transmission of unsolicited commercial or advertising material, chain letters, press releases or other junk-mail of any kind.

11. The unauthorised transmission to a third party of confidential material concerning the activities of the college or the personal data of other data subjects.
12. Downloading email attachments from people you don't know - these may contain viruses.
13. The transmission of material that infringes the copyright of another person, including intellectual property rights.
14. Activities that unreasonably waste staff effort or networked resources, or activities that unreasonably serve to deny service to other users.
15. Activities that corrupt or destroy other users' data or disrupt the work of other users.
16. Creation or transmission of any offensive, obscene or indecent images, data or other material.
17. 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, gender identity, 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.

<u>Unacceptable use of the internet</u>

18. Creation, transmission or distribution of offensive, obscene or indecent images, speech or material.
19. Creation, transmission or downloading and distributing material which infringes copyright regulations.
20. Transmission of commercial or advertising material, or political lobbying.
21. Activities which waste staff time or networked resources, including participation in "Chat Rooms".
22. Destruction of other people's data.
23. Wilful downloading or uploading of any form of computer virus.
24. 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.

25. Personal financial gain or advertising.
26. Pirating of software/files.

Software, copyright and downloading

27. 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.
28. Software available on the Group 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 Director of Digital.
29. Users should not import non-text files or unknown messages onto the Group's system without having them scanned for viruses.
30. 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 IT via TopDesk.
31. Users have a duty to ensure all software updates are installed as soon as possible after notification of release and must be installed with 14 days. This applies both to college devices and personal devices used to access systems.

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. 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.

Relevant policies and procedures for students

- Data Protection Policy
- Safeguarding and Preventing Extremism and Radicalisation Policy
- Online Safety Procedure
- Password Policy for Staff and Students
- Student Disciplinary Procedure
- Student Code of Conduct

Part C – Staff

In addition to the terms in parts A and B, staff must follow these additional guidelines to protect sensitive data. Staff accounts may have access to more sensitive information, while students and guests primarily have access to their own data.

1. Users must not purchase new IT software or hardware for business purposes. All such purchases must only be made by IT. In all cases, the risks of processing data on new software or hardware must be assessed by carrying out a Data Protection Impact Assessment.
2. Saving personal, sensitive data (special category of personal data) or corporate data on personal devices (USBs, hard drives, personal 'phones, personal cloud storage etc.) is prohibited. IT staff can provide guidance on how to encrypt and store and send personal and sensitive data securely e.g. via a OneDrive link, if normal methods are not usable.
3. Users must only use Group approved systems for the processing of business and personal data.
4. Users must be professional, respectful and factual in their communications via email or Teams. Remember that any personal data may be disclosed to a data subject under the terms of a data subject access request.
5. EKC Group systems are for the processing of data related to EKC Group. Staff and students should not therefore use EKC Group systems for their personal use.
6. 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 report it through TopDesk so that the matter can be investigated. Suspicious emails can be reported by using the 'report phishing' button, except from when using shared email boxes, in which case staff members should contact It through TopDesk.
7. 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.
8. Facebook, Twitter etc. can be used for promotional purposes via official EKC Group channels and must adhere to the Social Media Best Practice Guidelines. (Twitter, Facebook, TikTok etc)
9. If a curriculum area or service area wishes to set up a social media account such as Facebook, Twitter, WhatsApp or other, permission must be sought from the relevant Marketing Lead within each business unit. 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 Group into disrepute or be offensive to the viewer. Guidance on what can be posted on these accounts is available from the Marketing Lead. Useful information about the safe and secure use of IT and social networking can be found on the Get Safe Online website and the National Cyber Security Centre.

10. Staff must not use personal devices or channels to communicate with students or store information about students e.g. photographs, student data etc.
11. Staff may only use EKC Group issued Microsoft email addresses, 365 products and repositories (i.e. one drive, teams and SharePoint) and any other systems/software that have been approved by IT for business purposes.
12. The use of other non EKC Group issued systems or personal emails accounts e.g. Google drive, DropBox, WhatsApp, Gmail, Yahoo Mail etc. is not permitted. Staff should **not** use their personal email address to share commercial, student or staff data. This is because:
    12.2 The Group is required by law to have in place measures to protect personal and corporate data. When such data is processed via other systems, it is not possible to protect the data.
    12.3 Staff may not consent to their personal data being shared with others e.g. a personal mobile number on a WhatsApp group used for business purposes.
13. Microsoft products and repositories must be used in accordance with defined security settings.
14. Staff must comply with safety and security protocols when engaging in online working or learning. Teaching and student support staff must also ensure that students understand and comply with online protocols.
15. When remote working/working from home, staff must ensure that they are working safely and securely and in accordance with relevant procedures.
16. When a member of staff leaves EKC Group's employment, any reference to current employment with EKC Group on social media, such as LinkedIn must be removed.
17. All IT equipment must be returned by the user when they leave EKC Group. Managers are responsible for collecting equipment and returning it to IT.
18. Staff are only permitted to use personal mobile phones and tablets for business when compliant and joined to the colleges mobile device management (MDM) system. Only supported channels (Teams/Email) can be used to communicate with students. Staff must not use personal laptops/desktop running Windows/MacOs/Linux for college purposes.
19. All devices used to connect are subject to audit and any request as a result should be complied with, within 2 working days. Eg sending screen shots of certain settings screens on a staff personal mobile.

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 EKC Group; whilst the Group 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 a College/business unit's leadership team following due process. Instances where the Group may have to interrogate emails are as follows.

- Unexpected or prolonged absence of a member of the Group 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 or whistleblowing investigations.
- To investigate possible criminal activity.

20. 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 Group 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.
21. Staff should not create email congestion by sending trivial messages or unnecessarily copying emails or replying to all. Unnecessary emails should be deleted regularly to prevent over-burdening the system. Files should also be deleted from deleted and sent items.
22. 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.
23. 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 EKC Group as gross misconduct.
24. Emails sent outside the Group should include EKC Group's 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 EKC Group.

25. To ensure compliance with the Freedom 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 contact details of a colleague dealing with issues arising in their absence.

26. 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. People services 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 one to one basis rather than by email to assist their integration back into the working environment.

27. Staff who have left the organisation will have their accounts deleted, however, an auto response will be added for two weeks to ensure any contacts made are responded to appropriately. After this time the account will close. This message will be as follows:

    'Thank you for your email. I have now left EKC Group. Please contact enquiries@EKCGroup.ac.uk, who will be able to respond to your query.'

28. Staff should be mindful of when emails are sent. The Group places no expectation on staff to send or respond to emails during holidays, out of working hours, weekends or whilst on leave of absence for whatever reason.
29. Emails should not be used in favour of face to face or telephone communication.
30. Opinions and discussions regarding other staff members' performance or behaviour should not be transmitted via email, or Teams
31. Emails to 'all staff' that relate to cross-Group matters must be approved by the Executive team; if approved for circulation they will be posted by the Executive support team. Emails to 'all staff' that relate to individual College/business unit matters must be approved by the relevant College/business unit lead.
32. Staff must be careful not to send emails which disclose the personal data of others to someone who is not authorised to receive it. The content of emails must therefore be checked carefully before they are sent and the recipient's address should be double checked.
33. Staff should avoid sending attachments in an email and should link to the source document wherever possible. If a file needs to be transmitted it should be sent via a OneDrive link
34. Emails and attachments which include personal/special category data must not be sent externally via email. A OneDrive link should be used in all circumstances.
35. Where a data breach has occurred and an email recipient has received information which was not intended for them and/or contains personal or special category data about other data subjects, IT may delete the email from the user's account to prevent further dissemination of the data. This can only be done if the email was sent to/from an EKC Group account.
36. 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 EKC Group as gross misconduct.

Use of Teams and online working

All the principles applied to the use of emails and the internet apply. Staff and students should also comply with all applicable procedures when working online. In addition, users must:

37. Request the set-up of a Teams site via IT. Teams will be set up in private mode as default unless there is a clear business rationale for making the Team public.

38. Teams owners are accountable for ensuring the security of the Teams site and the integrity of the data within the site; this includes authorising owners of the site (for business continuity purposes there must be at least 2 owners of teams sites which serve as document repositories), legitimate users to access the site, deleting users where they no longer need access, setting document retention periods and granting access to specific folders/data within the site.
39. When recording in Teams, verbal consent will need to be obtained from the participants.

Social media

Social media/networking (Facebook, LinkedIn, Twitter, blogs, wikis etc.) can be a valuable tool in communicating 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 Group 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 Group 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:

40. 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.
41. 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.
42. The broadcasting of personal data/information without a person's consent and knowledge is prohibited.
43. 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 Group business only.
44. The relevant Marketing Lead within each Business Unit 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.
45. 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.
46. Staff should not engage in communications about potentially sensitive or political topics or legal matters relating to the college.
47. Any communication via social media must always be respectful and accurate and avoid the possibility of incorrect assumptions being made.

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 EKC Group for the cost of the call(s)/text(s).

Cloud Computing

Cloud providers are likely to store and move data around multiple servers situated in a number of jurisdictions. This can result in a breach of Data Protection legislation unless there are adequate security measures in place for personal data. Compliance may be achieved if 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 non-Microsoft product cloud-based applications.

Relevant policies and procedures for staff

- Data Protection Policy
- Remote, Mobile and Homeworking Procedure
- Safeguarding and Preventing Extremism and Radicalisation Policy
- Online Safety Procedure
- Staff Code of Conduct
- Password Policy for Staff and Students