Communications Policy

Version 1.0

Number 1.11

Policy Number 7.17

Updated on 12/03/2024

Review Date 12/03/2025

Responsible Person: Human Resource Officer

Linked policies:

- General Data Protection Regulation policy
- 11b. Data Privacy Notice
- 29. Privacy Notice & Consent
- Employee Handbook:
- Email & Internet Policy
- Disciplinary Procedures Policy

Contents

1 Communications Strategy

1.1. UK Graduate (‘UKG’, or the ‘College’) aims to ensure that communications are conducted legally, professionally, effectively, and respectfully to the benefit of all stakeholders through the utilisation of appropriate channels.

1.2. The College upholds the right to freedom of speech and academic freedom for all staff, students, and stakeholders. We recognise that in some circumstances, comments may be deemed offensive even though they may be permitted under the law. In these instances, we exercise the right to use discretion when balancing the need for tolerance of opinion and comment, with respect for others.

1.3. The College distinguishes between internal communications conducted between staff and students, and external communications conducted between staff and external bodies including partner organisations, awarding bodies, regulators, UK funding bodies, the public and media outlets.

1.4. The College organisational chart illustrates communication requirements for reporting and accountability purposes. Managers report to the Managing Director; Functional Officers report to Functional Managers; and Tutors/Assessors report to the Quality and Standards Manager.

1.5. Formal Committee meetings ensure effective management and quality assurance systems of all College activities are effective, monitored and enhanced through periodic action and development planning.

2 Staff Obligations

1.6. Staff are expected to communicate honestly with integrity and to respect the rights and privacy of others in relation to electronic communication and information. The College reserves the right to store all electronic communication and files conducted by stakeholders to College email accounts and other College data sharing platforms.

1.7. Every employee will be given access to the Internet as appropriate to their job needs. All device and network access will be through passwords, and no individual is permitted onto the system using another employee’s, students’ or other stakeholder’s password. Stakeholders are not permitted to share their password with anyone. Individuals will be allowed to set their own password and must change them as frequently as requested by the system set-up requirements.

1.8. Staff must not breach intellectual property rights in their communications through inappropriate downloading, copying, possessing, or distributing material from the internet. For guidance purposes, staff are permitted to print and distribute up to 5% of printed or digital material that is copyrighted if they include a reference to the author if the College has Copyright certification granting permission. Staff can print and distribute any material that is classified as ‘open source’.

1.9. You must ensure that when sending emails using College email accounts that you are careful to check your facts and ensure accuracy and appropriateness of language. Any email can be produced in court and used against you or the College in any legal proceedings.

1.10. You are a representative of the College if you are speaking with someone in-person, using a video conferencing platform, on the telephone, or writing to them in email or other form. As a College representative you should avoid expressing personal opinions if you know or believe those opinions may be contrary to your line manager or the Managing Director.

1.11. You must avoid using the College email or name in any activity that may lead to disciplinary or legal action.

1.12. You will face disciplinary action by the College if you are found to have been sexist, racist, defamatory, or unlawful in any of your communications whilst working for or on behalf of the College. If you are in doubt about how to communicate, take advice from your line manager. If you receive communications that are inappropriate or potentially illegal, inform you manager.

3 Internal Communications

1.13. Formal internal communications are maintained through quarterly Board and Committee meetings that include:

Academic Board
(Audit & Risk Committee)
Quality & Standards Committee
- Admissions Committee
- Course Committees

Operations Committee
- Finance Committee

Business Development Committee
- Marketing & Recruitment Committee

1.14. The Academic Board has overall academic management of the College.

1.15. The Audit & Risk Committee provides overall independent oversight of the College's compliance with internal policies and procedures and with external regulations and presents and Audit and Risk Assessment to the Academic Board.

1.16. The Quality & Standards Committee is responsible for overseeing the quality and standards of all services including admissions, courses, and student support services.

1.17. The Admissions Committee reports on admissions to the Quality and Standards Committee.

1.18. The Operations Committee is responsible for procuring, managing and maintaining the resources and facilities of the College including staff recruitment, training, support, appraisal and payroll, campus facilities, equipment and furniture and learning resources.

1.19. The Finance Committee is responsible for managing the College's finances and budgets and for maintaining the College Ledger and liaising with the College accountant for the productions of the annual accounts.

1.20. The Business Development Committee is responsible for ensuring sustainable growth and development of the College in line with its Strategic Plan, Business Plan, and organisational objectives.

1.21. The Marketing and Recruitment Committee is responsible for developing and implementing the Marketing Plan and Student Recruitment Plan in accordance with the Access and Participation Statement and Business Plan

4 Personal Telephone Calls/Mobile Phones

1.22. The College receives many enquiries by telephone. Incoming/outgoing personal telephone calls are allowed on site but should be kept to a minimum. Personal mobile phones should be switched off or 'on silent' during working hours and only used during authorised breaks.

5 Use of Email

1.23. **UK Graduate use:** Staff should always use the "Bcc" box when mailing to groups whenever the members of the group are unaware of the identity of all the others (as in the case of marketing mailing lists), or where they judge that the membership of the group of one or more individuals should perhaps not be disclosed to the others (as in the case of members of a staff benefit scheme), because if they use the "Cc" box each recipient is informed of the identity (and in the case of external recipients, the address) of all the others. Such a disclosure may breach any duty of confidence owed to each recipient, breach the Company's obligations under the General Data Protection Regulation and Data Protection Acts or may inadvertently disclose confidential business information such as a marketing list. This applies to both external and internal e-mail. If staff are using the students' College email address, they may use their own judgement on whether it is acceptable to Cc emails or invitations to join an online lesson. However, when using personal email addresses in group emails, they should always Bcc them.

1.24. **Receiving work-related documents:** If an important document has been emailed, staff should telephone to confirm that the e-mail has been received and read. Considering the security risks inherent in web-based email accounts, staff must not email business documents to their personal web-based accounts. They may send documents to a student or colleagues account if they have permission to do so. However, under no circumstances should they send sensitive or highly confidential documents to a personal web-based e-mail account (e.g., Yahoo, or Hotmail), even if they are asked to do so.

1.25. **Personal use:** The College accepts that staff may occasionally use College email for their own personal purposes. This is permitted on condition that staff behave appropriately as set down in this policy and that staff accept that the College may need to monitor their communications. The College's facilities or email may not be used in connection with the operation or management of any business apart from UK Graduate business, unless staff have been given permission for this by their line manager.

1.26. Staff must ensure that their use of email use does not:

- Involve anything illegal
- Involve accessing or transmitting pornography or on-line gambling
- Include bullying, harassment, or other form of written abuse
- Involve transmitting information and/or software in breach of copyright
- Involve posting confidential information about any other person.
- Cause unwarranted expense or liability to the College or its stakeholders
- Impact negatively on the College in any way
- Interfere with or take priority over their work for UK Graduate apart from obvious exceptions such as when there may be health or family emergencies staff must attend to.

6 Use of Internet

1.27. The College accepts that staff may occasionally use internet for their own personal purposes. This is permitted on condition that all the procedures and safeguards detailed in this policy are complied with and their use of the internet does not interfere with the performance of their duties.

1.28. Care must be taken in the use of information accessed through the Internet. Whenever staff access a web site, they should always comply with the terms and conditions governing its use. Most information is unregulated, and as such it may not be accurate.

1.29. The use of the Internet to access and/or distribute any kind of offensive material, or material that is not work-related, leaves an individual liable to disciplinary action which could lead to dismissal.

1.30. Staff, students, or other stakeholders must not:

- Use any images, text or material which are copyright-protected, other than in accordance with the terms of the license under which you were permitted to download them
- Introduce packet-sniffing or password-detecting software
- Seek to gain access to restricted areas of the college's network
- Access or try to access data which they know or ought to know is confidential
- Introduce any form of computer virus
- Carry out any hacking activities

7 Use of Video Conferencing Platforms

1.31. The College may sometimes runs blended and distance learning classes online using video conferencing platforms such as Microsoft Teams or Zoom. The College also uses these platforms to host or join meetings internally with College staff or stakeholders and externally with partners or other organisations. When hosting or participating in an online lesson or representing the College in a meeting, staff are expected to maintain the same standards of conduct as detailed in this policy.

1.32. In addition, staff are expected to comply with the following whenever possible:

- Ensure that UKG logo displays are up to date.
- Make sure that they have appropriate equipment to communicate effectively online: laptop with audio/video and good internet connection.
- Turn on video and audio so that people can see and hear them, but make sure they are sitting in a place where there is nothing inappropriate that someone else may see.
- Make sure that they are dressed appropriately in accordance with the College dress code
- Use mute to cut out background noise, if necessary, when they are listening and not speaking
- If a programme is being delivered through blended or distance learning, staff and students must check their College email every day and respond to any email from a student, colleague, line manager or senior staff on the same day if possible or the next day the latest.
- In the presence of students or external bodies including meetings with partner organisations, staff should be respectful to each other and avoid derogatory remarks, arguments, or disagreements as much as possible. You may correct inaccuracies when it is constructive to do so and does not place a colleague in a compromising position. All disagreements should be addressed internally wherever possible, and not when external people are present. This does not include

8 Virus Protection Procedures

To protect the College from virus contamination in its software system you must observer the following:

- Only authorised staff should have access to the College's computer equipment.
- Only authorised software may be used on any of the College's computer equipment.
- Unauthorised access to the computer facility may result in disciplinary action.
- Unauthorised copying and/or removal of computer equipment/software may result in disciplinary action, such actions could lead to dismissal.
- No software may be brought onto or taken from the College's premises without prior authorisation.
- No unauthorised software including public domain software, magazine cover disks/CDs or Internet/World Wide Web downloads can be used on the College's devises
- New software must be checked and authorised by technical staff before general use.
- Standard testing procedures must be used to check all software for viruses before use.

9 System Security

All confidential information should be secure, password protected, retained on a needs only basis, used only for the purposes it is needed and not disclosed to any unauthorised third party that does not need it.

The College's system or equipment must not knowingly be used in any way which may cause damage or overloading, or which may affect its performance or that of the internal or external network.

10 Working Remotely

1.33. When working remotely (e.g. from home) staff must:

- Use passwords to protect any College-related work so that no other person can access it.
- Position themselves so that their work cannot be overlooked by any other person.
- Take reasonable precautions to safeguard the security of the College's laptop computers and any computer equipment on which they use, and keep their passwords secret
- Inform the police and UK Graduate as soon as possible if any device they have used for UKG work has been stolen or gone missing.
- Ensure that any work which they do remotely is saved on the company system or is transferred to the College system as soon as possible.

11 Monitoring of Communications by the Company

1.34. The College may randomly monitor staff communications to ensure they are:

- Carrying our work for the College
- Complying with the College Policies and Procedures
- Complying with UK law
- Meeting required standards and quality of service
- Not conducting unauthorised communications
- Maintaining effective communications.

1.35. From time to time the Company may monitor telephone, e-mail, and internet traffic data (i.e. sender, receiver, subject; non-business attachments to e-mail, numbers called and duration of calls; domain names of web sites visited, duration of visits, and non-business files downloaded from the internet) at a network level (but covering both personal and business communications). This includes monitoring of any additional accounts that staff may be requested to set up for the purposes of performing their work tasks, which are subject to the same rules as their work email account. Information acquired through such monitoring may be used as evidence in disciplinary proceedings.

1.36. Sometimes it is necessary for the College, to access staff communications during their absence, such as when they are away because they are ill or on holiday.

12 Data Protection

1.37. When using College communications facilities, many staff will inevitably be involved in processing personal data as part of their job. Data protection is about the privacy of individuals and is governed by the General Data Protection Regulation (GDPR) and its implementation in the current Data Protection Act 2018.

1.38. Whenever and wherever staff are processing personal data for the College they must keep this confidential and secure, and they must take particular care not to disclose such data to any other person (whether inside or outside the Company) unless authorised to do so. Staff should not use any such personal data except as authorised by the College for the purposes of their job. If in doubt, ask your line manager.

1.39. The Data Protection Act gives every individual the right to see all the information which any data controller holds about them. Bear this in mind when recording personal opinions about someone, whether in an e-mail or otherwise. Try to ensure all personal remarks are relevant, appropriate, accurate and justifiable.

1.40. The Data Protection Act states that it is a criminal offence to obtain or disclose personal data without the consent of the data controller. "Obtaining" here includes the gathering of personal data by employees at work without the authorisation of the employer. Staff may be committing this offence if without authority of the Company: they exceed their authority in collecting personal data; they access personal data held by the College; or they pass data on to someone else (whether inside or outside the Company).

13 Use of Social Networking Sites

1.41. Any work-related issue or material that could identify an individual who is a student, teacher, work colleague or any other stakeholder, which could adversely affect the College or its relationship with any stakeholder must not be placed on a social networking site. This means that without express approval from the data controller, work-related matters must not be placed on any such site at any time either during or outside of working hours and this includes access via any computer equipment, mobile phone, or PDA.

14 Confidentiality

1.42. Employees are not permitted to register with sites or electronic services in the company's name without the prior permission of their line manager. They are not permitted to reveal internal company information to any sites, be it confidential or otherwise, or comment on company matters, even if this is during after-hours or personal use. The company confidentiality policy applies to all electronic communication and data.

15 Policy Compliance and Reviews

If staff fail to comply with this policy they may face disciplinary action. Staff must consult their line manager if there is anything in this policy they do not understand. The Policy and Procedures will be reviewed annually but may be amended at any time if the need arises. Stakeholders will be informed of any amendments.