ARTS UNIVERSITY BOURNEMOUTH (AUB)

Communication Protocols

---

1. Introduction

1.1 This document summarises the communication protocols from AUB policies and guidelines which reflect current legislation and offer support to staff and students, enabling them to communicate in a professional and appropriate manner.

1.2 It provides guidance to ensure that communication channels which are made available to users including email, telephone, blogs and message boards, are used appropriately for the purposes of the University.

1.3 Communication plays an essential role in the conduct of the University which reflects on staff and students, both individually and collectively as members of the University. This document will aid understanding of communication protocols and offer guidance in using communication tools.

1.4 Guidelines and policies can be found on the intranet as indicated throughout the document. It is the responsibility of staff and students to maintain awareness of policies and guidelines and to access them as required.

1.5 These protocols apply to anyone using the Arts University Bournemouth's communication network, including staff and students, but also any visitors, volunteers or temporary workers.

2. General Principles (Behaviour / professionalism / acceptable use)

2.1 You must use information technology and communication facilities sensibly, professionally, lawfully, in a way that is consonant with your duties and with respect for your colleagues and for the University.

2.2 Internet and email are extremely easy and informal ways of accessing and disseminating information, however this also means it is easy to send out ill-considered statements. All messages you send electronically should demonstrate the same professionalism as other communication channels.

2.3 You must not use these channels to do or say anything which would be subject to disciplinary or legal action in any other context, such as sending any discriminatory (on the grounds of a person's age, disability, ethnicity, gender, religion or belief or sexual orientation), defamatory, or other unlawful material, including material that is designed to be, or could be construed as, bullying or harassing by the recipient.

2.4 You are not allowed to create, display, produce or circulate material which is illegal, likely to cause offence or which promotes terrorism. Where access to such material is deemed necessary, permission must be sought from the Deputy Vice-Chancellor.

2.5 Should notification be received from the police that our systems are being used to publish terrorist material, the Deputy Vice-Chancellor will instruct the Head of DCS to remove the material within two days of notification as required by law. The University will conduct a review of the material and how it came to be published: the review will be chaired by the Deputy Vice-Chancellor.

2.6 Some information relating to our staff and students and our business operations is confidential and must be handled in accordance with the Data Protection Act. You must ensure that this information is not left on a computer screen or paper documents left open on a desk for others to see: the information must be kept securely at all times.

2.7 When posting, copying, processing, downloading, uploading, and distributing material from the internet you must abide by copyright law as laid down in the Copyright, Designs and Patents Act 1988.

2.8 Any means of communication that include expressions of opinion, intention or unsubstantiated fact in an email or social networking sites may be binding and result in you or the University

facing legal action. Insert a disclaimer in emails or on your blog when you are expressing personal opinions to make it clear that they are not those of the University.

2.9 If you identify any material which you consider to be offensive, or otherwise prohibited by this policy, you should report it immediately by emailing acforscutt@aub.ac.uk

.

3. Data Protection

3.1 The Data Protection Act gives every individual the right to see all information which any data controller holds about them. You should bear this in mind when recording personal opinions about someone, whether in an email or otherwise. Personal remarks and opinions must be made or given responsibly, be relevant and appropriate, accurate and justifiable.

3.2 Training in Data Protection issues is given to all new staff on their University AUB induction day. If you are unsure of what is required or you need guidance in data protection, you should contact AC Forscutt, Compliance Officer.

4. Security

4.1 You must maintain a secure complex password. Passwords must be 8 characters long and include capitals and numbers e.g. Pa55word

4.2 Keep your system passwords safe and do not disclose them to anyone. If you have a legitimate reason to access other users' resources you must obtain permission from that other user. If you have mistakenly disclosed your password to anyone you must change your password immediately.

4.3 You must not download or install software from external/third party sources without prior authorisation from DCS to ensure compliance with software licence agreements.

The following documents are the full policies and guidelines for further reference:

Acceptable Use Policy

5. Mobile Devices (iPhones / Mobile) & Text Communication

5.1 AUB mobile devices are allocated to named employees for business use only. You are responsible for their use and must ensure that your devices are maintained safely and securely at all times.

5.2 You must report any lost or stolen device immediately to the ServiceDesk so that the device can be barred or wiped remotely. If the device is returned / found please inform the ServiceDesk immediately.

5.3 Any SMS Text messages you send out should be professional in tone and maintained for future audit purposes or to deal with any queries that might arise.

6. Remote Working

6.1 AUB procedures apply to the use of any computer systems, desktops, laptops, mobile devices and also your own computer equipment for whenever you are working on University business (working remotely).

6.2 You must ensure that AUB equipment, passwords, work and documents are kept secure. Inform the police and DCS immediately if any equipment containing AUB work/information is lost or stolen.

6.3 Any work which you do remotely must be saved on the University system or transferred it as soon as reasonably practicable

7. Use of Electronic Mail

7.1 You must use the AUB email address when communicating and ensure that you maintain any correspondence for future reference to ensure an audit trail.

7.2 Consider the target audience of your message – is email the appropriate communication channel? Would a more focused distribution group be more effective rather than an “all student“ or “all staff” email?

7.3 Ensure you describe the essence of the message clearly and concisely and use the subject line effectively.

7.4 You must ensure you have reviewed the file size of any attachments you send, and used compression tools/techniques where appropriate (resolution in images, zip archiving etc)

8. Web Applications and Services

8.1 You should conduct yourself ‘professionally’ when contributing to content-sharing sites, blogs, message boards and social networking (eg Facebook) on the Internet. In particular, avoid revealing personal details about yourself or others, and do not display offensive material that will be associated with yourself or the University.

8.2 Your profile may identify you as being associated with the University and your views could potentially be taken as a position of the University and not as your own personal opinion. You should therefore state a disclaimer in your profile which expresses that "these are my own personal views and not those of the Arts University Bournemouth.” If your comments on another person’s blog are contentious, you should consider similar wording.

8.3 When using online communities or collaborative tools, respect your peers. Tone of voice can easily be misinterpreted via the written word; use fact and reasoned argument to support your opinion.

9. Monitoring of communications by the University

9.1 The University is ultimately responsible for all business communications but subject to that, will, so far as possible and appropriate, respect your privacy and autonomy while working. The University may monitor your business communications for reasons which include:

9.1.1 ensuring that staff adhere to AUB business procedures, policies and contracts

9.1.2 compliancy with any legal obligations

9.1.3 maintaining the effective operation of AUB communications systems

9.2 The University will monitor telephone, email and internet traffic data (i.e. sender, receiver, subject; non-business attachments to email, numbers called and duration of calls; domain names of websites visited, duration of visits, and files downloaded from the internet). This will also include email content at a network level (but covering both personal and business communications). For the purposes of maintaining your own personal privacy, you need to be aware that such monitoring might reveal sensitive personal data about you.

9.3 Sometimes it is necessary for the University to access your business communications during your absence, such as when you are away because you are ill or while you are on holiday. If you have not made arrangements for this, a senior manager will authorise DCS to give access to an appropriate person.

9.4 All incoming emails are scanned by DCS on behalf of the University using virus-checking software. The software will also block unsolicited marketing email (spam) and email which have potentially inappropriate attachments. If there is a suspected virus in an email which has been sent to you, the sender will automatically be notified and you will receive notice that the email has not been delivered because it may contain a virus.

10. Compliance with this policy:

10.1 Failure to comply with this policy may result in disciplinary action being taken against you.

Staff

10.2 Staff who are suspected of failing to comply with this policy will be subject to the provisions of the Disciplinary and Dismissal Procedure. The University reserves the right to suspend access to certain services without prejudice pending the outcome of a disciplinary investigation and hearing. The outcomes of the Disciplinary and Dismissal Procedure will include a range of possible actions, as determined by the manager hearing the case, and may include the withdrawal of permission to use University equipment for personal purposes. In the most serious cases, the outcome may be summary dismissal.

10.3 The following are examples of matters that will be treated as gross misconduct capable of resulting in summary dismissal:

10.3.1 Revealing confidential information about the University in a personal online posting. This might include revealing information relating to AUB staff, students, policies, financial information or internal discussions. Consult your manager if you are unclear about what might be confidential.

10.3.2 Bringing the University into disrepute which may be by criticising or embarrassing it, its staff or its students in a public forum (including any website). You should respect the reputation of the University and the privacy and feelings of others at all times. If you have a genuine complaint to make about a colleague or the workplace you should follow standard University procedures.

10.3.3 You should note that behaviour which breaches the University Equality Statement, the Safeguarding Policy, or the Data Protection Policy, will always be considered to be extremely serious.

Students

10.4 Students who are suspected of failing to comply with this policy will be subject to the provisions of the Student Disciplinary Procedure. The University reserves the right to suspend access to certain services without prejudice pending the outcome of a disciplinary investigation and hearing. The outcomes of the Student Disciplinary Procedure will include a range of possible actions, as determined by the manager hearing the case, and may include the withdrawal of permission to use University equipment for personal purposes. In the most serious cases, the outcome may be the immediate termination of studies.

10.5 The following are examples of matters that will be regarded as sufficiently serious that they may result in the termination of studies:

10.5.1 Revealing confidential information about the University in a personal online posting. This might include revealing information relating to AUB staff, students, policies, financial information or internal discussions. Consult your course leader if you are unclear about what might be confidential.

10.5.2 Bringing the University into disrepute which may be by criticising or embarrassing it, its staff or its students in a public forum (including any website). You should respect the reputation of the University and the privacy and feelings of others at all times. If you have a genuine complaint to make about a member of staff or a fellow student, or the University in general, you should follow standard University procedures.

10.5.3 You should note that behaviour which breaches the University Equality Statement, or Data Protection Policy, will be always be considered to be extremely serious.

10.6 Please note that the procedures and policies outlined in this document, and in any related policy, may be reviewed or changed at any time. You will be alerted to important changes and updates will be published on our intranet.

10.7 If there is anything in this policy that you do not understand, please discuss it with your manager (for staff) or course leader (for students) in the first instance.

Policy edition: September 2018