UNIVERSITY OF Southampton

Electronic Communications Policy

1. INTRODUCTION

1.1 University of Southampton email and computer facilities are provided by the University and supported by iSolutions and made available to users for the purposes of the business of the University. A certain amount of limited and responsible personal use by users is also permitted. All use of our communications facilities is governed by the terms of this policy, and if our rules and procedures are not adhered to, then use of our facilities may be curtailed or withdrawn and disciplinary action may thereafter follow. Any breach of this policy may lead to disciplinary action being taken against you and serious breaches may lead to summary dismissal.

1.2 At the University, communication plays an essential role in the conduct of our business. How you communicate with people not only reflects on you as an individual but also on us as an institution. We value your ability to communicate with colleagues, students, fellow academics and outside bodies, and we invest substantially in information technology and communications systems which enable you to work more efficiently. We trust you to use them responsibly.

1.3 This policy applies to all individuals working for the University who use our communications facilities, whether academics, employed within the Schools or within Professional Services, full-time, part-time or fixed-term employees, visitors, contract staff, temporary staff, or employees working remotely.

1.4 Although the detailed discussion is limited to use of email and internet facilities, the general principles underlying all parts of this policy also apply to any other forms of electronic communications including telephone communications, fax machines, copiers and scanners. Note that some elements of personal use of the University's communications facilities are specifically addressed below. Please read this policy carefully.

2. GENERAL PRINCIPLES

2.1 You must use the University's information technology and communications facilities sensibly, professionally, lawfully, and consistently with your duties, with respect for your colleagues, and students and for the University and in accordance with this policy and the University's other rules and procedures.

2.2 In particular, you must abide by the University's computing regulations and iSolutions regulations, all of which may be found on the website under the iSolutions heading within SUSSED.

2.3 Confidential information relating to students, staff and the University's affairs must not be disclosed to unauthorized parties. You must treat our paper-based and electronic information with utmost care.

2.4 Many aspects of communication are protected by intellectual property rights which are infringed by copying. Downloading, uploading, posting, copying, possessing,

processing and distributing material from the internet may be an infringement of copyright or of other intellectual property rights.

2.5 Particular care must be taken when using email, blogs or internal message boards as a means of communication because all expressions of fact, intention and opinion in an email may bind you and/or the University and can be produced in court in the same way as other kinds of written statements.

2.6 The advantage of the internet and email is that they are extremely easy and informal ways of accessing and disseminating information, but this means that it is also easy to send out ill-considered statements. All messages sent on email systems or via the internet should demonstrate the same professionalism as that which would be taken when writing a letter or a fax. You must not use these media 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 sex, race, disability, age, sexual orientation, religion or belief), defamatory, or other unlawful material (for example, any material that is designed to be, or could be construed as, bullying or harassment by the recipient). If you are in doubt about a course of action, take advice from your supervising line manager.

2.7 Although the University's information technology and communications systems are provided for the purposes of our business, we accept that you may occasionally want to use them for your own personal purposes. This is permitted on the condition that all procedures and rules set out in this policy are complied with. Be aware however that if you choose to make use of our facilities for personal purposes, and while the University will respect items marked as personal as far as possible, you should not expect complete privacy because the University may need to monitor communications and use of its facilities for the reasons set out in 9.1.

2.8 Nothing in this policy shall be interpreted as precluding a member of staff from making a protected disclosure.

3. USE OF ELECTRONIC MAIL

3.1 Generally

3.1.1 Do not amend any messages received.

3.1.2 Do not access any other person's in-box or other email folders nor send any email purporting to come from another person. The only exception to this is where you have been authorized to access someone else's email for legitimate purposes connected to the University's operations, such as enabling someone to access your email while you are absent or enabling an assistant to respond to emails under your direction and on your behalf.

3.1.3 If you copy an email to others, it may breach the Data Protection Act if it reveals all the recipients' email addresses to each recipient (e.g. in the case of marketing and mailing lists).

It can also breach duties of confidentiality (e.g. in the case of internal emails to members of a staff benefit scheme). Accordingly, it may be appropriate to use the 'Bcc' (blind carbon copy) field instead of the 'Cc' (carbon copy) field when addressing an email to more than one recipient. If in doubt, seek advice from your line manager.

3.2 Business use

3.2.1 In light of the security risks inherent in some web-based email accounts, you must not email business documents to your personal web-based accounts.

3.3 Personal Use

3.3.1 You will greatly increase the privacy of any personal email by complying with the procedures set out in item 3.3.3 below.

3.3.2 Under no circumstances may the University's facilities be used in connection with the operation or management of any business other than that of the University unless express permission has been obtained from your line manager. (This includes private consultancy work carried out under the terms of the '30 day rule' referred to in the University's Consultancy Policy, as opposed to consultancy work carried out through University channels).

3.3.3 All personal email you send from University facilities should be marked PERSONAL in the subject heading, and all personal email sent or received must be filed in a separate folder marked "Personal" in your inbox should you wish to retain it after reading. All email contained in your inbox and your sent items box are deemed to be business communications for the purposes of monitoring (see item 9.4).

You must ensure that your personal email use:

(a) does not interfere with the performance of your duties;

(b) does not take priority over your work responsibilities;

(c) is minimal and limited to taking place substantially outside of normal working hours (i.e. during any breaks which you are entitled to or before or after your normal hours of work);

(d) does not cause unwarranted expense or liability to be incurred by the University;

(e) does not have a negative impact on the University in any way; and

(f) is lawful and complies with this policy.

3.3.4 As with any correspondence made using the University's electronic facilities, you can delete personal email from the live system, but they will have been copied (perhaps many times) onto the backup tapes and in that form will be retained indefinitely. It would be a very difficult, costly and time-consuming exercise to sift all those tapes in order to delete an individual's personal email, and if we were to agree to attempt this, it would be at our convenience, and only on the basis that all the very considerable costs involved were paid in advance by the person making the request.

3.3.5 By making personal use of our facilities for sending and receiving email you signify your agreement to abide by the conditions imposed for their use, and signify your consent to the University monitoring your personal email in accordance with item 9 of this policy.

4. USE OF INTERNET AND INTRANET

4.1 Bear in mind at all times that, when visiting a website, information identifying your PC may be logged. Therefore any activity you engage in via the internet may affect the University.

4.2 We recognise the need for individuals to have to carry out some personal tasks during working hours, e.g. for internet banking or online shopping, and this is permitted subject to the same rules as are set out for personal email use in item 3.3.3 of this policy.

4.3 The University does not sanction the installation of additional software for personal use. Software needed for the purposes of your research or other University duties can be installed provided this has been authorised from within your School or Service.

4.4 You are strongly discouraged from providing your University email address when using public websites for non-business purposes, such as online shopping. This must be kept to a minimum and done only where necessary, as it results in you and the University receiving substantial amounts of unwanted email.

4.5 Access to certain websites may be blocked during normal working hours. If you have a particular business need to access such sites, please contact iSolutions.

4.6 Prohibited Activities

You must not, without the prior authorisation of either the Director of iSolutions or Head of Legal Services:

4.6.1 introduce packet-sniffing or password-detecting software;

4.6.2 seek to gain access to restricted areas of the University's network;

4.6.3 unless you have been authorized to do so, access or try to access data which you know or ought to know is confidential;

4.6.4 carry out any hacking activities

4.6.5 intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software

4.7 For your information, breach of items 4.6.1 to 4.6.5 (inclusive) above, would not only contravene the terms of this policy but could in some circumstances also amount to the commission of an offence under the Computer Misuse Act 1990, which creates the following offences:

4.7.1 unauthorised access to computer material i.e. hacking;

4.7.2 unauthorised modification of computer material; and

4.7.3 unauthorised access with intent to commit or facilitate the commission of further offences.

5. MISUSE OF THE UNIVERSITY'S FACILITIES AND SYSTEMS

5.1 Misuse of the University's facilities and systems, including its telephone, email and internet systems, in breach of this policy will be treated seriously and dealt with in accordance with the University's disciplinary procedure. In particular, viewing, accessing, transmitting, posting, downloading or uploading any of the following

materials in the following ways, or using any of the University's facilities, will amount to gross misconduct capable of resulting in summary dismissal (this list is not exhaustive):

5.1.1 material which is sexist, racist, homophobic, xenophobic, pornographic, paedophilic or similarly discriminatory and/or offensive;

5.1.2 offensive, obscene, derogatory or criminal material or material which is liable to cause embarrassment to the University and any of its staff or bring the reputation of the University and any of its staff into disrepute;

5.1.3 any defamatory material about any person or organisation or material which includes statements which are untrue or of a deceptive nature;

5.1.4 any material which, by intent or otherwise, harasses the recipient;

5.1.5 any other statement which is designed to cause annoyance, inconvenience or anxiety to anyone;

5.1.6 any material which violates the privacy of others or unfairly criticises or misrepresents others;

5.1.7 confidential information about the University and any of its staff or students;

5.1.8 any other statement which is likely to create any liability (whether criminal or civil, and whether for you or the University);

5.1.9 material in breach of copyright and/or other intellectual property rights;

5.1.10 impersonation of another individual or purporting to be representing the University or another administrative entity, whether real or fictitious.

5.1.11 online gambling; or

5.1.12 unsolicited commercial or advertising material, chain letters or other junk mail of any kind.

If the University has evidence of the examples of misuse set out above it reserves the right to undertake a more detailed investigation in accordance with its disciplinary procedures.

An exception will be allowed for material that has genuinely been obtained for the purposes of legitimate academic research that is related to your area of study and where the acquisition of such material has been made known to the School in advance. It is recognised that academics will sometimes need to download material that could fall into one of the categories stated above. A member of staff involved in such research areas would be acting sensibly in making clear his or her intention to download such material and the reasons for this before proceeding, to reduce the possibility of criminal investigation by an external body.

6. INFORMATION AND SYSTEM SECURITY

6.1 Security of our IT systems is of paramount importance. It is vitally important that we are vigilant at all times to prevent unauthorised access to our information systems or unauthorised disclosure of information. If at any time we need to rely in court on any information which has been stored or processed using our IT systems it is essential that we are able to demonstrate the integrity of those systems. Every time

you use the system you take responsibility for the security implications of what you are doing.

6.2 The University's system or equipment must not 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.

6.3 Keep all confidential information secure, use it only for the purposes intended and do not disclose it to any unauthorised third party.

6.4 Keep your system passwords safe. Do not disclose them to anyone. Those who have a legitimate reason to access other users' inboxes must have University authorization to do so and be given permission from that other user.

6.5 If data is highly confidential, you should consider additional measures to prevent others from accessing the data without authorization, such as password protection.

6.6 Copies of confidential information should be printed out only as necessary, retrieved from the printer immediately, and stored or destroyed in an appropriate manner.

6.7 You should not download or install software from external sources without having first

6.7.1 received the necessary authorisation from your line manager;

6.7.2 ensure that the software has not been downloaded illegally, and that the correct licence has been obtained where appropriate; and

6.7.3 checked the terms and conditions of use to ensure that these do not present any risk to the University or its systems.

6.8 Unless it falls within the list of permitted items authorised by iSolutions, no external device or equipment, including discs and other data storage devices, should be run on or connected to the University's systems without the prior notification to and approval of iSolutions.

6.9 You should always exercise caution when opening emails from unknown external sources or where, for any reason, an email appears suspicious.

7. WORKING REMOTELY

7.1 This part of the policy and the procedures in it apply to your use of our systems, to your use of our laptops, and also to your use of your own computer equipment or other computer equipment (e.g. client's equipment) whenever you are working on the University's business away from the University's premises (working remotely).

When you are working remotely you must:

7.1.1 protect any work which relates to the University's business so that no other person can access your work;

7.1.2 take reasonable precautions to safeguard the security of our equipment, and keep your passwords secret;

7.1.3 inform iSolutions as soon as possible if either a the University laptop in your possession or any computer equipment on which you do the University's work, even if this is personal IT equipment, has been lost or stolen; and

7.1.4 ensure that any work which you do remotely is saved on the University's system or is transferred to our system as soon as reasonably practicable.

7.2 Pocket computers, mobile phones and similar hand-held devices are easily lost or stolen so you must protect access to any such devices used by you on which is stored any personal data of which the University is a data controller or any information relating our business, our clients or their business.

8. PERSONAL BLOGS AND WEBSITES

8.1 This part of the policy and procedures in it apply to content that you publish on the internet (e.g. your contributions to blogs, message boards and social networking or content-sharing sites) even if created, updated, modified or contributed to outside of working hours or when using personal IT systems.

8.2 The University recognise that you may wish to publish content on the internet for legitimate purposes connected with academic study or research, or with trade union activities. For the avoidance of doubt, such activities that are not related to these matters are expressly prohibited during work time or using the University's systems.

8.3 If you post any content to the internet, written, vocal or visual, which identifies, or could identify, you as a member of the University staff and/or you discuss your work or anything related to the University, the University expects you, at all times, to conduct yourself appropriately and in a manner which is consistent with your contract of employment and with the University's policies and procedures. It should be noted that simply revealing your name or a visual image of yourself could be sufficient to identify you as an individual who works for the University.

8.4 If a blog posting clearly identifies that you work for the University and you express any idea or opinion then you should add a disclaimer such as "these are my own personal views and not those of the University".

8.5 The following matters will be treated as gross misconduct capable of resulting in summary dismissal (this list is not exhaustive):

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

8.5.2 Save for the legitimate exercise of academic freedom, making a statement that is likely to bring the University into disrepute or criticising or damaging the reputation of the University, its students or its staff 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 workplace matter the correct procedure is to raise a grievance using the University's grievance procedure.

8.6 If you think that something on a blog or a website could give rise to a conflict of interest and in particular concerns issues of impartiality or confidentiality required by your role then this must be discussed with your line manager.

8.7 If someone from the media or press contacts you about your online publications that relate to the University, the University's press office should be informed. (Please also note the Media Protocol which may be found via SUSSED on the Communications website).

8.8 Online publications which do not identify the author as a member of the University staff and do not mention the University and are purely concerned with personal matters will normally fall outside the scope of the University's communications policy.

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 providing evidence of business transactions;

9.1.2 ensuring that the University's procedures, policies and contracts with staff are adhered to;

9.1.3 complying with any legal obligations;

9.1.4 monitoring standards of service, staff performance, and for staff training;

9.1.5 accessing emails for reasons related to the University's business while you are absent from work (provided that reasonable efforts have been made to contact you in advance to notify you of use, if contact is appropriate);

9.1.6 preventing or detecting unauthorised use of the University's communications systems;

9.1.7 preventing or detecting fraudulent or criminal activities or other misconduct that could give rise to action under the University's disciplinary procedures; and

9.1.8 maintaining the effective operation of the University's 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) at a network level (but covering both personal and business communications) for the purposes specified at item 9.1. For the purposes of your maintenance of your own personal privacy, you need to be aware that such monitoring might reveal sensitive personal data about you. For example, if you regularly visit websites which detail the activities of a particular political party or religious group, then those visits might indicate your political opinions or religious beliefs. By carrying out such activities using the University's facilities you consent to our processing any sensitive personal data about you which may be revealed by such monitoring.

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. Unless your mailbox settings are such that the individuals who need to do this already have permission to view your inbox, access will be granted only with the authorisation of your Head of School or Head of Professional Service (or in their absence, their deputy)

9.4 Any emails which are not stored in your "Personal" folder in your mailbox and which are not marked PERSONAL in the subject heading will be treated, for the purpose of availability for monitoring, as business communications since we will have no way of

knowing that they were intended to be personal (unless this is absolutely clear from the subject heading). Therefore you must set up a rule to automate the routing of personal email to your personal folder – ask iSolutions for guidance on how to do this. Furthermore, there is a risk that any person authorised to access your mailbox may have their own preview pane option as a default setting, which would reveal the content of any of your personal email not filed in your "Personal" folder, whether or not such email are marked PERSONAL. It is up to you to prevent the inadvertent disclosure of the content of personal email by filing your personal email in accordance with this policy. In particular, you are responsible to anybody outside the University who sends to you, or receives from you, a personal email, for the consequences of any breach of their privacy which may be caused by your failure to file your personal email.

9.5 In certain very limited circumstances we may, subject to compliance with any legal requirements, access email marked PERSONAL or which appears to be personal. Examples are when we have reasonable suspicion that they may reveal evidence of unlawful activity, including instances where there may be serious misconduct or a breach of a contract with the University.

9.6 All incoming email is scanned on behalf of the University, using virus-checking software. The software may 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 is not going to be delivered to you because it may contain a virus.

10. DATA PROTECTION

10.1 As a member of the University who uses our communications facilities, you will inevitably be involved in processing personal data for the University as part of your job. Data protection is about the privacy of individuals, and is governed by the Data Protection Act 1998. This Act defines, among others, terms as follows:

10.1.1 "data" generally means information which is computerised or in a structured hard copy form;

10.1.2 "personal data" is data which can identify someone, such as a name, a job title, a photograph;

10.1.3 "processing" is anything you do with data – just having data amounts to processing; and

10.1.4 "data controller" is the person who controls the purposes and manner of processing of personal data – this will be the University, in the case of personal data processed for the business.

10.2 Whenever and wherever you are processing personal data for the University you must keep it secret, confidential and secure, and you must take particular care not to disclose them to any other person (whether inside or outside the University) unless authorised to do so. Do not use any such personal data except as authorised by the University for the purposes of your job. If in doubt get help from our Data Protection Officer within Legal Services or your line manager.

10.3 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 email or otherwise. It is another reason why personal remarks and opinions must be made or given responsibly, and they must be relevant and appropriate as well as accurate and justifiable.

10.4 For your information, section 55 of the Data Protection Act provides 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. You may be committing this offence if without authority of the University: you exceed your authority in collecting personal data; you access personal data held by the University; to control it or you pass them on to someone else (whether inside or outside the University).

10.5 While the University is a data controller of all personal data processed for the purposes of our business, you will be a data controller of all personal data processed in any personal email which you send or receive. Use for social, recreational or domestic purposes attracts a wide exemption under the Data Protection Act, but if, in breach of this policy, you are using our communications facilities for the purpose of a business which is not the University's business, then you will take on extensive personal liability under the Data Protection Act.

10.6 To help you understand and comply with the University's obligations as a data controller under the Data Protection Act you may be offered, and you may also request, training. Whenever you are unsure of what is required or you otherwise need guidance in data protection, you should consult our Data Protection Officer. Information about our data protection policies can be found via SUSSED.

11. COMPLIANCE WITH THIS POLICY

11.1 Failure to comply with this policy may result in disciplinary action being taken against you under the University's disciplinary procedures, which may include summary dismissal, and/or in the withdrawal of permission to use the University's facilities. If there is anything in this policy that you do not understand, please discuss it with your line manager.

11.2 Please note that the procedures and policies outlined in this policy, 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 the website.

11.3 The University reserves the right to recover from you any costs which may be incurred as a result of a failure to comply with any of the provisions of this policy.

11.4 Where the evidence that a criminal offence may have been committed as a result of any misuse of the University's information technology and communications systems, this may be referred to the police or the appropriate regulatory authority.

12. OWNERSHIP OF THIS POLICY

12.1 This policy shall be the responsibility of iSolutions who have the task of monitoring it. Any query relating to the policy, or information about any possible breach of the policy shall be referred to the Director of iSolutions (who shall refer the matter to the Head of Legal Services where appropriate).

May 2010.