Ravensbourne Acceptable Use Policy

1. Introduction

Ravensbourne depends heavily on its Communications and Information Technology services for its research, teaching and administrative activities. These services are funded on condition they are used for legitimate, authorised purposes, and Ravensbourne may be required from time to time to demonstrate to external auditing bodies that it has mechanisms in place to manage, regulate and control them.

2. Purpose

The main purpose of these regulations is to define what constitutes acceptable use; to encourage the responsible use of facilities; to maximise the availability of resources (equipment, infrastructure and staff) for legitimate purposes; and to minimise the risk of misuse from inside or outside Ravensbourne.

These regulations incorporate the acceptable use policy of our service provider, JANET(UK) the United Kingdom Education & Research Networking Association, which manages network connections between Universities and Colleges and the Internet. The full text of their policy can be found at: JANET Acceptable Use Policy (AUP)

There are also various national and European Community laws and directives that govern the use of ICT, and others that make explicit reference to ICT. These are mentioned in more detail later. Ravensbourne has a duty to bring these to the attention of its staff and students.

If you are not sure whether something you are planning to do might contravene these regulations, check first with your line manager (in the case of staff) or tutor (in the case of students), or seek help from the ICT Help Desk before proceeding.

3. Scope

These regulations cover the use of all ICT services and facilities provided by Ravensbourne or by third parties on behalf of Ravensbourne. For the purposes of clarification, these include, but are not limited to: all computers irrespective of ownership when connected to the

Ravensbourne communications network; services run by Information Communication and Technology (ICT) Information Systems (IS) which may be used by any member of Ravensbourne.

All users of these services must be registered with IS; facilities and systems operated by departments for academic research, teaching and administration. Arrangements for use of

these facilities are made through the department concerned and are normally restricted to its own staff and students; content hosted on Ravensbourne's ICT facilities which is accessible via the internet by members of the public; services operated by third parties on behalf of Ravensbourne.

Software obtained under an educational licence agreement may also be subject to the terms of these regulations (see, for example, section 3.1 below). They do not, however, apply to other organisations whose traffic RUL relays by formal arrangement (such as the Janet(UK) ' sponsored' sites), unless the terms of an arrangement stipulate otherwise. In the case of sponsored sites, regulations will be established by agreement.

4. Policy Statement

4.1.Authorised Use

4.1.2 In these regulations "authorised use" is defined as: for students, use properly associated with the Ravensbourne programme of study or course for which a student is registered; and reasonable personal use; for employees, use in the course of or properly and directly associated with their employment; and reasonable personal use; for sessional staff, use properly associated with their appointment; and reasonable personal use; for users who are neither staff nor students, use restricted to those purposes specified in the case made for registration.

4.1.3 Reasonable personal use is defined as incidental and occasional use which does not: disrupt or distract the individual from the efficient conduct of Ravensbourne business (i.e. due to volume, frequency, time expended or time of day used); involve accessing, downloading, storing or sending offensive or inappropriate material or information, or is such as to amount to a criminal or civil offence examples of which are listed in Regulation 3(d); restrict the use of those systems by other legitimate users; risk bringing Ravensbourne into disrepute or placing the College in a position of liability; add significantly to running costs and breach the Regulations set out in paragraph 3 Any use that falls outside of these definitions is prohibited and may lead to Ravensbourne disciplinary procedures being invoked, with penalties that could include suspension from the use of all Ravensbourne computing facilities for extended periods. Serious cases may lead to disciplinary action, up to and including dismissal without notice and may expose you to court proceedings attracting both criminal and civil liability. You will be held responsible for any claims brought against Ravensbourne and any legal action to which Ravensbourne is, or might be, exposed as a result of your unauthorised use.

4.2 Regulations

ICT users must:

4.2.1 Respect the copyright of all materials and software that are made available by Ravensbourne service providers and third parties for authorised use; Users must not make, run or use unlicensed copies of software or data.

They should only download data or datasets where they are explicitly permitted to do so. They must abide by the CHEST Code Of Conduct For The Use Of Software Or Datasets (see https://www.chest.ac.uk/user-obligations/), the terms of the JISC Model Licences (see https://www.jisc-collections.ac.uk/Support/How-Model-Licences-work/), Copyright Law (Copyright, Designs and Patents Act 1988) and by any specific conditions of use imposed by the owners or suppliers of software or data. In particular users should be aware that, unless otherwise stated, software and datasets provided by Ravensbourne should only be used for Ravensbourne educational purposes.

4.2.2 Familiarise themselves with and comply with the requirements of the Data Protection Act and Ravensbourne policy, most especially the obligation to notify Ravensbourne's Data Protection Officer of any relevant data holdings; Data Protection laws protect individuals against the unauthorised use or disclosure of their data. Ravensbourne is registered with the UK Data Protection authorities. The processing, misuse or disclosure of an individual's data outside Ravensbourne's registration may amount to a criminal offence. Further information is set out in the appropriate Staff or Student Handbook.

4.2.3 Comply with the Computer Misuse Act of August 1990 which makes activities such as hacking or the deliberate introduction of viruses a criminal offence; Hacking is defined here as the unauthorised use of a computer system (locally or through a network), or the use of resources that have not been allocated, with intent to access, modify or damage another's files or system files, or to deny service to legitimate users, or to obtain or alter financial or administrative records, or to facilitate the commission of a crime.

4.2.4 Have the written approval of their Head of Department where activities which might be subject to legislation are carried out in pursuit of legitimate, approved academic research (for example, work involving the use of images which may be considered obscene or indecent, or research into computer intrusion techniques).

4.2.5 Take all reasonable precautions to prevent the introduction of any virus, worm, Trojan Horse or other harmful program to any computer, file or software;

4.3 ICT users must not:

4.3.1 Use material or programs in a way which is unlawful, defamatory or invasive of another's privacy;

4.3.2 Use the ICT services and facilities in such a way as to risk or to cause loss, damage or destruction of data or breaches of confidentiality of data;

4.3.3 Use the ICT services and facilities in a way which infringes any patent, trademark, trade secret, copyright, moral right, confidential information or other proprietary right of any third party

4.3.4 Jeopardise the provision of services (for example by inappropriate use of bulk e-mail, or by recreational use that deprives other users of resources);

4.3.5 Publish, create, store, download, distribute or transmit material that is offensive, obscene, indecent or unlawful. Such materials will always include, but at Ravensbourne's discretion may not be limited to, items deemed to be offensive, obscene, indecent or unlawful under The Obscene Publications Act 1959, The Sex Discrimination Act 1975, The Race Relations Act 1976, Disability Discrimination Act 1995, Part-Time Workers (Prevention of Less Favourable Treatment) Regulations 2000, Fixed-Term Employees (Prevention of Less Favourable Treatment) Regulations 2002, Employment Equality (Sexual Orientation) Regulations 2003, Employment Equality (Religion or Belief) Regulations 2003, Harassment Act1997, Employment Equality (Age) Regulations 2006, The Protection of Children Act 1978, The Public Order Act 1986, the Criminal Justice and Public Order Act 1994 and the Terrorism Act 2006.

4.3.6 Use ICT facilities in a way that brings or could bring Ravensbourne into disrepute. This includes associating Ravensbourne with external facilities such as Web sites that could bring Ravensbourne into disrepute by association, for example by embedding Ravensbourne email addresses in such sites, or by providing hyperlinks from Ravensbourne web sites to such sites;

4.3.7 Disclose passwords to others, or use accounts or passwords belonging to others, or otherwise to circumvent registration procedures; The term "password" is here taken to refer to any authentication credential issued by Ravensbourne, and includes both hardware tokens and cryptographic keys. Users will be held personally liable and may be subject to disciplinary proceedings for any misuse of their account resulting from the disclosure of passwords to others.

4.3.8 Access or attempt to access computers or computing services at Ravensbourne or elsewhere for which permission has not been granted, or facilitate such unauthorised access by others;

4.3.9 Attempt to circumvent any firewall or software designed to protect systems against harm;

4.3.10 Interfere or attempt to interfere with or destroy systems or software set up on public facilities (this includes loading or attempting to load unauthorised software on to any Ravensbourne ICT facilities);

4.3.11 Interfere with, disconnect, damage or remove without authority any equipment made available for use in conjunction with any Ravensbourne ICT facilities;

4.3.12 Set up equipment to provide services that they are not competent to administer, especially if such services result in security vulnerability or exposure to misuse;

4.3.13 Use mobile phones, smoke, eat or drink in public cluster rooms;

4.3.14 Interrupt teaching sessions when a cluster room has been booked for this purpose. Ravensbourne does not tolerate discrimination or harassment in any form whatsoever. This principle extends to any information distributed via any Ravensbourne ICT system or via the Internet. You may not store on or transmit from any system any material which discriminates or encourages discrimination or harassment on racial or ethnic grounds or on grounds of gender, sexual orientation, marital status, age, ethnic origin, colour, nationality, race, religion, belief or disability. [Please also bear in mind the Ravensbourne policy on discrimination and harassment.] Breaches of this policy will lead to disciplinary action. In the event that you receive or become aware of obscene, indecent, offensive, inflammatory, discriminatory or socially offensive material, you should notify the relevant person set out in paragraph Failure to comply with these regulations may lead to disciplinary action, up to and including dismissal from Ravensbourne without notice and may expose you to court proceedings attracting both criminal and civil liability. You will be held responsible for any claims brought against Ravensbourne and any legal action to which Ravensbourne is, or might be, exposed as a result of your unauthorised use.

4.2 Conditions of Use

4.2.1 Use of Ravensbourne ICT facilities is subject to the following conditions. Additional conditions may apply to locally managed systems; it is the responsibility of those managing such systems to make their users aware of any local regulations.

4.2.2 The facilities (including software) are provided entirely at the risk of the user. Ravensbourne will not be liable for loss (including any loss of software, data or other computer functionality or any economic, consequential or indirect loss), damage (including damage to hardware, software or data) or inconvenience arising directly or indirectly from the use of the facilities, except where statutory health or safety matters are involved.

4.2.3 Whilst Ravensbourne's information security policy requires providers of computing facilities to employ appropriate security measures to prevent unauthorised access to, alteration, disclosure, destruction or accidental loss of personal and other data, Ravensbourne cannot and does not give any warranties or undertakings to the user about security, confidentiality or integrity of data, personal or other. The same applies to any other electronic material submitted to or processed on facilities provided or managed by Ravensbourne or otherwise deposited at or left on its premises.

4.2.4 Ravensbourne accepts no liability for any loss (including any loss of software, data or other computer functionality or any economic, consequential or indirect loss), or damage (including damage to hardware, software or data or the invalidation of any warranty agreement) to equipment not owned by Ravensbourne as a consequence of any work carried out on such equipment by members of staff (or students acting in the capacity of members of staff), whether authorised or not.

4.2.5 Ravensbourne accepts no liability for any loss (including any loss of software, data or other computer functionality or any economic, consequential or indirect loss), or damage (including damage to hardware, software or data or invalidation of any warranty agreement) to equipment not owned by Ravensbourne as a consequence of direct or indirect connection, whether authorised or not, to Ravensbourne networks. The user shall indemnify Ravensbourne for any loss or damage, whether direct or indirect, malicious or inadvertent, suffered or incurred as a consequence of the interconnection of any hardware or software not owned by or under the control of Ravensbourne with any IT system, hardware, software or data owned or controlled by Ravensbourne.

4.2.6 Ravensbourne reserves the right to inspect, monitor, copy and/or remove user data in order to investigate operational problems or for the detection and investigation of suspected misuse. This includes the authorised interception and monitoring of communications as provided for by The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, made under the Regulation of Investigatory Powers Act 2000.

4.2.7 Ravensbourne reserves the right to check for insecure and vulnerable systems and to block access to systems and/or services (ports) which place at risk the integrity of its network or services, or which may pose a threat to third parties.

4.2.8 Ravensbourne reserves the right to disconnect poorly managed equipment from the departmental LAN, or in extreme cases disconnect the departmental

LAN from the Ravensbourne network until the offending machine is disconnected or shown to be configured correctly.

4.3 Procedures for dealing with misuse or suspected security violations

4.3.1 In the event of suspected misuse of ICT facilities Ravensbourne reserves the right to suspend user accounts and to inspect, monitor, copy or remove users' files if necessary. Ravensbourne may also disconnect network services, including those to rooms in Halls of Residence and prevent access to the facilities without notice while investigations proceed.

4.3.2 Cases of misuse or abuse should be reported to ICT.

4.3.3 The Head of Department and Ravensbourne authorities, may be informed and will deal with the incident under the appropriate disciplinary procedures for students and staff. In some cases legal action may be taken and the Police informed. Ravensbourne reserves the right to disclose data or information about an individual's use of RUL's computing facilities to any appropriate or authorised third party (including the police) to assist in any further investigation.

4.2.4 If websites containing material that may be illegal are discovered, particularly material relating to children or the exploitation of children, Ravensbourne encourages its staff and students to make a report to the authorities named above or to the Internet Watch Foundation (IWF) hotline (http://www.iwf.org.uk) . The normal course of events is that the IWF will request that the Internet Service Providers (ISPs) in the UK will block that site. If this does not happen the IWF will inform the Police who may investigate the matter further.

4.2.5 Actual or suspected security violations should be reported immediately to the RUL Computer Security Team (e-mail support@rave.ac.uk). No attempt should be made to investigate security vulnerabilities unless or until appropriate authority has been obtained.