University Academy Keighley

The Use of ICT Systems Policy

‘Inspiring Education in the Bradford District’

CONTENTS

1.0 Roles and Responsibilities

1.1 The Principal is responsible to the Governing Body for ensuring the implementation of the agreed policy and in advising them of appropriate amendments. On an operational basis, the management, responsibility and evaluation of this policy is undertaken by the Assistant Principal – Specialism.

2.0 Suggested Audience:

All teaching and learning support staff

3.0 University Academy Keighley Mission Statement

'Inspiring Education in the Bradford District'

4.0 Introduction

4.1 The Governing Body recognises the use of ICT as an important resource for teaching, learning and personal development. It actively encourages staff to take full advantage of the potential for ICT to enhance development in all areas of the curriculum and academy administration. It is also recognised by the Governing Body that along with these benefits there are also responsibilities, especially for ensuring that children are protected from contact with inappropriate materials.

4.2 In addition to their normal access to the Academy's ICT systems for work-related purposes, the Governing Body permits staff limited reasonable use of ICT equipment and e-mail and internet facilities during their own non contact time as long as they are not:

- depriving students of the use of the equipment; and/or
- interfering with the proper performance of the staff member's duties.

4.3 Whilst the Academy's ICT systems may be used for both work-related and personal reasons the Governing Body expects use of this equipment for any purpose to be appropriate, courteous and consistent with the expectations of the Governing Body at all times.

4.4 The use of computer equipment, including laptop computers, which is on loan to staff by the Academy for their personal use at home is covered by this policy. Staff who have equipment on loan are responsible for its safekeeping, travelling to and from the Academy as well as at home, and for ensuring that it is used in compliance with this policy.

5.0 Guidance on the Use of Academy ICT Facilities

5.1 Whilst it is not possible to cover all eventualities, the following information is published as guidance for staff on the expectations of the Governing Body. Any non-conformance to this policy or operation outside statutory legal compliance may be grounds for disciplinary action being taken.

5.2 Further guidelines on the responsible use of ICT facilities are contained in the Bradford Council document 'Internet Access Policy for schools' (2001).

6.0 E-mail, Mobile phone technology and Internet Usage

6.1 The following uses of the Academy's ICT system are prohibited and may in certain circumstances amount to gross misconduct and could result in dismissal:

- to gain access to, and/or for the publication and distribution of inappropriate sexual material, including text and/or images, or other material that would tend to deprave or corrupt those likely to read or see it;
- to gain access to, and/or for the publication and distribution of material promoting racial hatred;
- for the purpose of bullying or harassment, or for or in connection with discrimination or denigration on the grounds of gender, race, disability or sexual orientation;
- for the publication and/or distribution of libellous statements or material which defames or degrades others;
- for the publication and distribution of personal data without either consent or justification;
- where the content of the e-mail correspondence is unlawful or in pursuance of an unlawful activity, including unlawful discrimination.
- to participate in on-line gambling;
- where the use infringes copyright law;
- to gain unauthorised access to internal or external computer systems (commonly known as hacking); and
- to enable or assist others to breach the Governor's expectations as set out in this policy.

6.2 Additionally, the following uses of Academy ICT facilities are not permitted and could lead to disciplinary action being taken:

- for participation in 'chain' e-mail correspondence;
- in pursuance of personal business or financial interests, or political activities (excluding the legitimate activities of recognised trade union representatives); and
- to access ICT facilities using another person's password, or to post anonymous messages or forge e-mail messages using another person's identity.

6.3 See appendix 3 for a copy of the University of Bradford's ICT Regulations policy which covers students from post 18 onwards.

7.0 Use of Academy ICT Equipment

7.1 Users of Academy ICT equipment:

- must not share and must treat as confidential any passwords provided to allow access to ICT equipment and/or beyond firewall protection boundaries;

- must report any known breach of password confidentiality to the Principal or nominated ICT Co-ordinator as soon as possible;
- must report breaches of this policy, including any inappropriate images or other material which may be discovered on the Academy's ICT systems;
- must not install software on the Academy's ICT systems, including freeware and shareware, unless authorised by the Academy's ICT Co-ordinator; and
- must comply with any ICT security procedures governing the use of systems in the Academy, including anti-virus measures.

8.0 Regulation of Investigatory Powers Act 2000

8.1 Ancillary to their provision of ICT facilities the Governing Body asserts the employer's right to monitor and inspect the use by staff of any computer and telephonic communications systems where there are grounds for suspecting that such facilities are being, or have been, misused.

*A guideline 'Responsible Computer Technology Use' will be made available to all users (see Appendix 1)

9.0 Review

9.1 The Assistant Principal - Specialism will work will all staff to ensure this policy is fully implemented. The Assistant Principal - Specialism will also monitor and review the development of this important policy and make a written report to the Governing Body on an annual basis.

10.0 Approval by the Governing Body and Review Date

10.1 This policy has been formally approved and adopted by the Governing Body at a formally convened meeting

Policy approved: _____

(Chair of Governing Body)

Date: _____

Date of Policy review: _____

11.0 Appendix1: Responsible Computer Technology Use

11.1 Guidelines for All Computer Technology Users

11.2 The computer system is owned by the Academy. This Responsible Computer Technology Use statement helps to protect students, staff and the Academy by clearly stating what use of the computer resources, including mobile phone technology, is acceptable and what is not.

- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- Irresponsible use will result in the loss of Internet access.
- Academy computer, mobile phone technology and internet use must be appropriate to the student's education or to staff professional activity.
- Copyright and intellectual property rights must be respected.
- E-mail should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers.
- Users are responsible for e-mail they send and for contacts made.
- Anonymous messages and chain letters are not permitted.
- The use of unmonitored chat rooms is not allowed.
- The Academy ICT systems may not be used for private purposes, unless the Principal has given permission for that use.
- Use for personal financial gain, gambling, political purposes or advertising is not permitted.
- ICT system security must be respected; it is a criminal offence to use a computer for a purpose not permitted by the system owner.
- Items can only be placed on the Academy website with authorisation from the Systems Manager
- Parental permission is required when publishing articles in publications and /or web sites that identify students.
- Students will be provided with information for raising awareness regarding safety on the Internet and cyber bullying through the curriculum and assemblies.

11.3 The Academy exercises its right to monitor the use of the Academy's computer systems, including access to web-sites, mobile phone technology, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the Academy's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. Further guidelines on the responsible use of ICT facilities are contained in the Bradford Council document 'Internet Access Policy for Schools' (2001) available from the Academy office.

12.0 Appendix 2: Policy on the Use by Staff of Academy ICT Systems

12.1 This declaration refers to the Governing Body's policy on the use of ICT systems (attached). A further copy can be obtained from the Academy office. If you experience any difficulty assessing the policy please raise the matter with the Principal.

12.2 All employees, supply agency staff, consultants and contractors are required to familiarise themselves with the contents of the policy on the use of ICT systems and sign the following declaration.

12.3 Declaration

You should sign two copies of this document, this copy to be retained with the policy for your personal record, and a copy to be stored by the Academy.

I confirm that I have been provided with a copy of the Academy's policy and guidance on the use of the Academy's ICT systems. Signed: Name: Date: Copy to be retained by the member of staff.

(cut here)

12.4 Declaration

You should sign two copies of this document, this copy to be stored by the Academy and one copy (above) to be retained with the policy for your personal record.

I confirm that I have been provided with a copy of the Academy's policy and guidance on the use of the Academy's ICT systems. Signed: Name: Date: Copy to be returned to academy office.

13.0 Appendix3: Regulation 21 on Use of University Computing Facilities and the Campus Network

- Note: this Policy is currently under review.
- Note: a descriptive commentary on this regulation follows below.

1. General

i. Access to the University Campus Network and use of computing facilities owned by the University are conditional on observance of the following Regulations.

ii. In the following sections, *facilities* is used as a general term encompassing the Campus Network and all computers and peripherals owned by the University and the information, data and software used or stored on them. This includes but is not limited to equipment or applications managed by the Computer Centre, by individual departments and throughout the University administration.

iii. Users of personally owned equipment connected on campus, in the Halls of Residence or through telephone or data services are bound by these Regulations if such use makes direct or indirect use of *facilities* and, in particular, the Campus Network.

iv. The term *appropriate manager* is used to mean the member of staff responsible for specified facilities. This includes the appropriate Dean of School, Head of Planning Unit or Department, or a member of staff with delegated responsibility.

v. The term *user* refers to any person that makes direct or indirect use of *facilities*.

2. Availability of facilities

i. *Facilities* are available for research or study approved by the University or for authorised administrative purposes to all staff and registered full and part-time students of the University. No person or persons may use *facilities* without prior authorisation from the *appropriate manager*.

ii. Other persons may be granted permission to use *facilities* on application to the *appropriate manager*. In the case of academic computing services, applicants must complete an External User Registration Form available from the Reception Desk in the J B Priestley Building.

iii. External User registration is also necessary for staff and students using the academic computing service for non-university work, which includes, but is not limited to, consultancies or private work undertaken for reward.

iv. Some programs and packages have been provided on education contracts restricting them to use by members of the University and more specifically to University research or study. If use by external users is permitted, it may incur additional charges.

v. External users will be invoiced for use of *facilities* and associated costs and are personally responsible for reimbursing the University.

3. Code of conduct

i. Authority to use *facilities* is given on the understanding that they are to be used only for the purpose authorised and only by the *user* or *users* authorised to use them. *Users* are personally responsible for the security of resources allocated to them and must not allow another to use their account without prior authorisation from the *appropriate manager*.

ii. *Users* must not cause any unnecessary noise or disturbance to others or use *facilities* in a way that results in a degradation or disruption of the service to others. In particular, distribution of computer viruses, electronic chain mail, computer games, use of Internet Relay Chat (IRC) or similar services are strictly forbidden unless authorised exceptionally by the *appropriate manager* for academic purpose.

iii. The consumption of food or drink and smoking are forbidden in equipment areas (e.g. workstation cluster rooms) and all other areas displaying appropriate notices.

iv. No *user* shall by any wilful or deliberate act jeopardise the integrity of *facilities*, or attempt to access, copy, modify, disseminate or make use of information, data or software without appropriate authorisation.

v. *Users* must treat as privileged any information, including software, which may become available to them intentionally or accidentally through the use of *facilities*. In particular, access to any information owned by another *user* is forbidden unless authorised by the owner and by the *appropriate manager*.

vi. *Users* accessing software, datasets or services available through University *facilities* must comply with licence agreements or contracts relating to their use and must not alter or remove copyright statements. Some items are licensed for educational or restricted use only. Details are available from the *appropriate manager*.

vii. Software must not be reverse engineered, de-compiled or incorporated into other programs or products without the express permission of the licensor or author as appropriate.

viii. The transmission, storage, promotion or display of offensive, defamatory or harassing material is strictly forbidden unless authorised exceptionally for legal academic purpose. In such cases the *user* must obtain prior written authority from the University and all appropriate external bodies and must comply with any conditions imposed.

ix. *Facilities* shall not be used to hold or process personal data except in accordance with the provisions of the Data Protection Act. Any person wishing to use *facilities* for such a purpose is required to inform the University Data Protection Officer in advance and comply with any restrictions that the University or the UK Information Commissioner may impose concerning the manner in which data may be held or processed.

x. *Users* must treat with respect equipment and services at other sites accessed through University *facilities* and are subject to regulations imposed by the respective service providers. All use of the academic network (JANET), direct or indirect, is bound by the JANET Acceptable Use Policy issued by UKERNA.

xi. *Users* must comply with the Code of Conduct for use of software and datasets adopted by the Joint Information Systems Committee of the Higher Education Funding Councils.

xii. *Users* must comply with the University Policy and Code of Practice on Information Security and Access.

xiii. *Users* producing material to be accessed through the University World-Wide Web Information Server must comply with the Code of Practice on World Wide Web Authoring issued by the World-Wide Web Editorial Board.

xiv. *Users* are not permitted to use *facilities*, in particular Electronic Mail, to propagate unsolicited materials, e.g. advertisements and promotions, unless authorised exceptionally by the University and *appropriate manager*.

4. Penalties

i. Regulations regarding holding, processing or disclosure of personal data are enforceable by law under the Data Protection Act.

ii. Regulations regarding unauthorised access or misuse of computing facilities are enforceable by law under the Computer Misuse Act.

iii. Regulations regarding copying of software and other material are enforceable by law under the Copyright, Designs and Patent Act.

iv. Regulations regarding the transmission, storage or display of obscene material are enforceable by law under the Criminal Justice and Public Order Act 1994 which amends the Obscene Publications Act 1956, the Protection of Children Act 1978 and the Telecommunications Act 1984 to extend their provisions to transmission over a data communications network.

v. Any person making unauthorised use of *facilities* or, through the use of networking, making unauthorised use of equipment or services at another site may be required to pay damages which may include, but are not limited to:

- resources used or incurred by such usage,
- repairs to or replacement of equipment and
- resources and time used in investigation.

vi. Any infringement of regulations may lead to temporary suspension of use of *facilities* by the *appropriate manager*. Students in breach of regulations will be reported to their tutor and Dean of School.

vii. The *appropriate manager*, within his or her discretion, may waive or vary a penalty if the circumstances warrant such action.

viii. Where the *appropriate manager* takes the view that the seriousness of a case or multiple offences constitute a breach of Statute 29 (Academic Staff) or Ordinance 16 (Conduct of Student Members of the University), the matter will be referred to

the Registrar and Secretary. If it is agreed that it warrants such action, formal disciplinary proceedings under Statute 29 or regulation 28 will be instituted.

Commentary on Regulation 21

Current University Regulations are published in the University Calendar available from Corporate & Central Services. University Regulation 21 covers use of all University computing facilities available across the campus and of the Campus Network. Current copies of both University Regulation 21 and the associated Code of Conduct follow this commentary. Additional copies are available from the J B Priestley Building Reception Office. Your attention is drawn to the fact that regulations may be amended from time to time but that they are available electronically, using the World-Wide Web Information Service.

The Code of Conduct (covering use of site licensed software and datasets) is the basis for most software site licences across the campus. All **employees and students of the University** are bound by both University Regulations and the Code of Conduct. If you use any of the applications available on University facilities, you are personally responsible for complying with the terms of the Code of Conduct and may be required to complete a separate Copyright Acknowledgement for some items of software.

If you are not a member of the University and wish to use site licensed software and datasets, you must complete an **External User Registration Form**. In addition, External Users must complete a Copyright Acknowledgement for each item of software or dataset and must have prior authorisation from the University through the Computer Centre (or appropriate manager) before using it. Some software may only be used for education and research and others incur additional licence or royalty payments. All use is again bound by University Regulations and the Code of Conduct.

Availability of Computing Resources

In order to use University computing resources you need a computer account. An account must only be used by the user to whom it was allocated. Group accounts are not normally provided and use of another computer user's account is not allowed without prior authorisation from the appropriate manager. In the case of central facilities, you need to apply to the Computer Centre for appropriate authorisation.

Users are responsible for their computer accounts and they must only be used for approved University work (see Regulation 21, paragraph 2i). This may include familiarising yourself with the network and services available through it, including communicating with fellow students through electronic means. *However, such privileges only extend to communication carried out in the spirit of Regulation 21 (see below, Computer Misuse).* In particular, University resources are not to be used for consultancies or private work unless a special account has been allocated for the purpose (see Regulation 21, paragraphs 2ii through 2iv).

Computing facilities at the University of Bradford and at other institutions are valuable resources which should be conserved. Users should utilise resources properly and intelligently to minimise the impact of their work on others. In particular, game playing, the use of 'chat' applications (e.g. IRC) and electronic chain mail are strictly forbidden (see Regulation 21, paragraph 3ii).

Please avoid obstructing the work of others by consuming inordinately large amounts of system resources (e.g. disk space, CPU time, network traffic or volume of output) particularly during peak times. If work is unsuitable for Bradford, it may be possible to use larger National Facilities.

Proprietary Rights

Copyright software must only be used in accordance with the Code of Conduct for Use of Software and Datasets. This has been adopted nationally by the Joint Information Systems Committee of the Higher Education Funding Councils and by the Committee of Vice Chancellors and Principals. In addition, Regulation 21 explicitly states that users should not acquire or make use of unauthorised copies of software or make unauthorised copies for themselves or others. Many of the software contracts for education and research could not be negotiated without a background of trust and respect for the rights of authors and publishers.

Because electronic information is volatile and easily reproduced this is especially easy in a network environment. The Computer Centre will strive to maintain adequate security and compliance with the terms of licence agreements and contracts and will take action against any violation of authorial rights, invasion of privacy or Trade Secret or Copyright violation. *If you use software or information illegally, you will be held personally responsible.*

Computer Misuse

In the context of paragraph 3v of Regulation 21, viewing or using another person's computer files, programmes or data without permission is not only unethical behaviour, it contravenes the Computer Misuse Act 1990. Modification of computer systems or software, in any unauthorised manner, is strictly forbidden. More generally, Users must not browse, access, copy or change files owned by others, including public files, without prior authorisation. This includes deleting or creating files in another's account.

Other examples of unauthorised use of the computing systems are:

1. distribution or use of invasive software, such as 'worms', 'Trojan Horses' and 'viruses';
2. attempting to gain access to any account not belonging to you, including attempts to identify user passwords on University facilities or those of other institutions;
3. use of University computing facilities as a staging ground to crack other systems;

4. deliberately or knowingly causing a system to fail or service to crash;
5. facilitating access to or the transmission, display or replay of material which may be considered offensive, defamatory or harassing in the context of the University Code of Practice on Personal Harassment (see paragraph 3viii);
6. random mailings or electronic chain letters;
7. playing games or use of IRC on University facilities;
8. distribution of messages of a commercial or political nature.

Privacy of Files and Electronic Mail

It is important that all users exercise caution when committing sensitive information to electronic media. University computing facilities are connected to both local area and national and international networks. They are accessible therefore to the academic community and beyond (through Internet). Although the University is taking steps to provide secure communication and storage of sensitive material, **it cannot guarantee confidentiality at present**. You are personally responsible for the confidentiality and security of your information, therefore. The safest recommendation currently is that you avoid using facilities connected to the academic network for sensitive information.

Electronic mail at the University of Bradford is as private as it can be. Attempts to read another person's electronic mail or other protected files are strictly forbidden and Computer Centre staff will not read mail or other files unless absolutely necessary in the course of their duties. However, routine maintenance or system administration may result in the contents of files or communications being seen inadvertently. The contents of such files will be treated by our staff as private information at all times but action will be taken if such mail or files fall into one of the unauthorised categories (e.g. contrary to Regulation 21 paragraph 3viii).

Security

Users should also be aware that the Computer Centre performs periodic security checks, including checking passwords. Guidelines on choice of a password are published frequently by the Computer Centre and are imposed by software. If easily guessed passwords are detected, the user will be notified. If the password is not changed within a short period, it will be changed by the Computer Centre to protect both the account and the facilities in general.

Finally, it is stressed that computing facilities at Bradford University are provided for your benefit. If you find a possible security breach or know of or suspect a hacking attempt, it is in your interest to report it to the Computer Centre. If you are unsure, report it anyway without trying to use it.