PHOENIX COLLEGE

USE OF ELECTRONIC SYSTEMS IN SCHOOLS POLICY

Reading Borough Council

Risk Management – Policy on the use of Electronic systems in Schools

CONTENTS

1. **INTRODUCTION**
2. **BACKGROUND – THE REASONS FOR THE POLICY**
3. **PURPOSE AND SCOPE OF THE POLICY**
4. **PERMITTED BEHAVIOUR**
5. **UNACCEPTABLE BEHAVIOUR**
6. **CONFIDENTIALITY OF INFORMATION**
7. **AUDIT, RECORD-KEEPING AND SCRUTINY**
8. **HUMAN RIGHTS ACT 1998**
9. **CONCLUSION AND FURTHER READING**

---

1. INTRODUCTION

This policy sets out a framework for staff and managers on the **permitted and prohibited** use of the Council's/schools electronic systems – a definition which includes all computer systems as well as the Council Intranet, Internet and e-mail systems, mobile telephones, pagers etc. It is intended to help and guide all staff as to what is acceptable usage and what is not and constitutes an addition to the Council's/schools Code of Conduct.

Whilst this policy emphasises what staff can do as well as what they cannot, it should be stressed that the restrictions in this policy, if breached, could lead to disciplinary action in accordance with the Council's/schools existing procedure for dealing with such matters.

Other guidance documents have been produced which give staff and managers advice on **'best practice'** in electronic systems usage as well as guidance on e-mail and Internet etiquette and **'housekeeping'**.
These supplementary documents **do not** form part of the Council's/schools Code of Conduct for staff – rather, they are issued to assist all staff to make more effective use of the systems and equipment currently available although they may also be used as a framework for discussion between managers and staff/teams on appropriate or acceptable methods of working.

This policy has been agreed between the Council/school and its recognised trades unions and constitutes an incorporated term of individual contracts of employment.

2. BACKGROUND – THE REASONS FOR THE POLICY

The use of electronic systems – especially the Internet and e-mail access - has greatly increased across society and within organisations over the past few years. All the projections point towards this trend continuing with increased business and personal use of these systems. The Council welcomes this development and has made a substantial investment in the provision of computer 'hardware' and 'software' tools (and other electronic systems) to assist and enhance the services that it provides to the local population. However, the introduction of these systems brings new challenges and disciplines that need to be incorporated within the procedures and polices that we adopt as an organisation.

On one hand there is the need to weigh the understandable desire of staff to use these systems for private as well as work activities. The continuing development of commercial aspects of the Internet (sometimes called 'e-commerce') as well as the growth in the medium of e-mail as a means of communication are developments in which employees of the Council will want to participate.

On the other hand there is the need to weigh the legal implications and technical costs involved in misuse of these systems. In the final analysis, electronic systems are tools of work, provided and paid for by the Council/school. It is important, therefore, that the integrity and efficiency of these systems is maintained whilst at the same time allowing staff reasonable opportunity to access these systems for their own use.

3. PURPOSE AND SCOPE OF THE POLICY

The **purpose** of this policy is –

a) To provide guidance to users of the Councils/schoo's electronic information systems on acceptable and unacceptable use of these systems and related equipment.

b) This policy is not designed to place unreasonable restrictions upon individuals in their use of these systems and equipment, but rather to –

- Protect all staff against the downloading and/or dissemination of offensive images and writing

- Ensure that private use of these systems and equipment does not hinder the effective working of members of staff and the service that they are employed to provide

- Ensure that the systems and equipment are kept secure from external and internal interference, sabotage or computer 'viruses'

- Keep the systems working at optimum efficiency and performance levels

- Protect the Council/school from legal action arising from misuse as well as liability for the actions of its employees and other users

c) Encourage the skills, confidence and development of staff and other users in using electronic equipment and systems while at the same time offering adequate protection to the Council/school and other users from the potential negative effects of e-mail and Internet media.

The **Scope** of the Policy:

This policy applies to **all users** of electronic hardware and software systems provided by Reading Borough Council and the school – whether this access and/or related equipment is provided directly by the Council/school or through contractors engaged by the Council/school for that purpose. This policy applies irrespective of the location of the electronic equipment and/or systems themselves.

Whilst the terms of the employment related aspects of this policy cannot be applied to users who are not employees of the Council/school, such users are expected to conform to (and abide by) the terms of this Policy in respect of 'Permitted Behaviour' and 'Unacceptable Behaviour' as set out below. To meet this requirement non-employee users may be asked to sign a declaration to this effect. **It is the responsibility of those Directorates with external users to devise and implement a strategy and system for doing this.**

4. PERMITTED BEHAVIOUR

You are allowed **reasonable access to the Council's/school's electronic systems for personal use.** Reasonable in this context is defined as activities that–

(a) do not detract from your overall work performance,

(b) are not related to a personal business interest and

(c) are conducted in accordance with this Policy and the related 'Best Practice' guides.

The factors that contribute to this assessment may vary from time to time and, therefore, you are encouraged to discuss these arrangements with your line manager in either individual supervision sessions or team meetings to obtain further guidance. There may be a need to reimburse the Council/school the costs involved in this use (i.e. in the case of the use of mobile phones) and details of these arrangements will be notified to you at the time of issue of this equipment.

The Council/school also accepts that organisations that are recognised to operate within the Council/school (such as Trades Unions) will have a need from time to time to

communicate with their members – on an individual or collective basis. Use of the e-mail and Intranet systems are permitted for such organisations within the framework of this Policy and the related guidelines referred to above.

5. UNACCEPTABLE BEHAVIOUR

The following is a list of behaviours when using the Council's/school's electronic systems that are **always unacceptable** and may lead to disciplinary action in accordance with the terms and the principles of the Council's Disciplinary Procedure. **Please note that this is not an exhaustive list, but it is indicative of the sort of behaviour that will not be tolerated.**

The downloading, transmission, re-transmission, display or other form of dissemination of material (either images or words) that could be regarded as:-

a) being harassing or offensive on the grounds of gender, sex, race, sexual orientation, disability, religion or age

b) defamatory or derogatory of individuals or organisations

c) inappropriate in a workplace context such as pornography – in either picture or written form

d) Non compliance with relevant laws on copyright and the Data Protection Act(s) (DPA) or Council polices and procedures issued to ensure compliance with such Acts and/or related Regulations.

e) Unauthorised transmission of confidential or private information about the business or personnel of the Council/school to people or organisations not authorised to receive it

f) Misuse of equipment which is defined as deliberate damage or sabotage of equipment or systems howsoever caused (i.e. through physical action or the use of software viruses) as well as deliberate failure to follow audit or technical instructions about the use of such equipment as may be issued by the relevant Council Departments/school from time to time

g) Unauthorised monitoring or interception of electronic files or messages; deliberately obtaining unauthorised access to systems or accounts; using 3rd party log-in's or passwords without permission; breaching, testing or monitoring IT system security measures; deliberate attempts to hide or disguise the identity of the sender of a message (or represent the sender as someone else)

h) Personal use of systems or equipment for non-work related activities that could be regarded as unreasonable – see definition of what is 'reasonable' behaviour above.

6. CONFIDENTIALITY OF INFORMATION

The Council/school undertakes not to make random audits of e-mail transmissions or Internet use unless this is for the purpose of cost analysis, resource allocation, or optimum technical management. Information or data arising from this work may be shared with the relevant Head teacher/line manager should the Department conducting the audit consider it necessary.

In addition, head teacher/line managers may, from time to time review an employee's electronic files, messages or Internet usage if there is prima facie evidence that an employee is –

(a) abusing the Council's/school's systems or equipment under one of the 'Unacceptable Behaviour' headings above, or;

(b) otherwise engaged in activities which contravene the Council's Code of Conduct, or;

(c) involved in activities which contravene a previously issued management instruction.

In order for this to be done, a line manager will need to present such evidence to the head teacher to obtain approval for a review or audit prior to this being carried out. This application and the approval (if given) should be recorded.

A member of staff (or other user) will be told that they are the subject of such an investigation as soon as it is reasonably practicable to do so – 'reasonably practicable' in this context is defined as 'at a time when such advice will not hinder or impede the progress of such an investigation'.

Staff should not assume, therefore, that their transmissions or electronic records are secure.

7. AUDIT, RECORD KEEPING AND SECURITY

Head teacher are responsible for introducing and maintaining systems that record the location of equipment issued to users of the Council's/school's electronic systems and the person(s) to whom this equipment has been issued. These records should be audited and updated from time to time. This requirement extends to equipment owned by the Council/school as well as equipment provided through a contract supplier, lease, loan or similar arrangement.

These record/audit systems should also record the users of 'non-standard' software used in conjunction with such equipment which is not issued through the Council's/school's IT section or IT provider.

As a minimum such an audit should be undertaken (and recorded) at least once every 12 months.

It is the responsibility of all staff who use electronic equipment, software and related systems to take reasonable care in protecting this equipment/systems from accidental damage, theft or misuse by 3rd parties.

8. HUMAN RIGHTS ACT 1998

This Policy conforms to the provisions and the principles of the Human Rights Act 1998

9.Conclusion & Further Reading

This policy sets out the framework of acceptable and unacceptable behaviour when using the Council's/school's electronic systems and equipment. Further guidance about use of these systems can be obtained from the following –

Systems and Equipment – Council IT Services
Staff discipline and counselling advice – Directorate Personnel Teams

Best Practice when using IT equipment/systems (including internet and email etiquette) – Council 'Use of Electronic Systems - Best Practice Guide'

Health and Safety Policy – Use of VDU's