Policy on School ICT and Communications Systems

PACT HR

Menston Primary School
Policy for School Staff

Approved by the Governing Body March 2015
This is an adoption of a Bradford LA Pact-HR policy
To be reviewed by the Finance and General Purpose Committee March 2016 or sooner if the council's policy is revised

City of Bradford MDC
www.bradford.gov.uk

Contents

1. Policy Statement

The Governing Body recognises the use of its ICT and communications facilities as an important resource for teaching, learning and personal development and as an essential aid to business efficiency. It actively encourages staff to take full advantage of the potential for ICT and communications systems to enhance development in all areas of the curriculum and school 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 material.

In addition to their normal access to the school's ICT and communications systems for work-related purposes, the Governing Body permits staff limited reasonable personal use of ICT equipment and email and internet facilities during their own time subject to such use:

- not depriving pupils of the use of the equipment

and/or

- not interfering with the proper performance of the staff member's duties

Whilst the school's ICT systems may be used for both work-related and for personal use, 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.

This policy document is to be issued to all staff on its adoption by the Governing Body and when new staff are provided with mobile phones and passwords giving access to the ICT network. It should be issued and read alongside The Use of Social Networking Sites Policy.

Policy Coverage

This policy covers the use by staff of all school-owned ICT and communications equipment, examples of which include:

- laptops, personal computers and tablets
- ICT network facilities
- personal digital organisers and handheld computers
- mobile phones and phone/computing hybrid devices
- USB keys and other physical and on-line storage devices
- Image data capture and storage devices including cameras, camera phones and video equipment

  This list is not exhaustive.

The policy covers the use of all ICT and communications equipment provided for work purposes and equipment which is on loan to staff by the school for their personal or study use.

2. The use of school ICT and Communications Facilities

Use of School ICT Equipment

Staff who use the school's ICT and communications systems:

- must use it responsibly
- must keep it safe
- 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 Headteacher or nominated ICT Co-ordinator as soon as possible
- must report known breaches of this policy, including any inappropriate images or other material which may be discovered on the school's ICT systems
- must report to the Headteacher any vulnerabilities affecting child protection in the school's ICT and communications systems
- must not install software on the school's equipment, including freeware and shareware, unless authorised by the school's ICT Co-ordinator/Headteacher/Primary Technology
- must comply with any ICT security procedures governing the use of systems in the school, including anti-virus measures
- must ensure that it is used in compliance with this policy
- must only use a password protected area of an encrypted USB pen drive issued by the school for portable document storage of school data.

Any equipment provided to a member of staff is provided for their personal use. Any use of the equipment by family or friends is not permitted and any misuse of the equipment by unauthorised users will be the responsibility of the staff member. School laptops/tablets are issued with Bitlocker USB ignition to prevent unauthorised access to school data.

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 breaches of this policy or operation of the school's equipment outside statutory legal compliance may be grounds for disciplinary action being taken.

Email and Internet and Communications Systems Usage

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

- to make, to gain access to, 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 make, to gain access to, and/or for the publication and distribution of material promoting homophobia or racial or religious hatred

- for the purpose of bullying or harassment, or for or in connection with discrimination or denigration on the grounds of gender, race, religious, disability, age or sexual orientation

- for the publication and/or distribution of libellous statements or material which defames or degrades others

- for the publication of material that defames, denigrates or brings into disrepute the school and/or its staff and pupils

- for the publication and distribution of personal data without authorisation, 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)

- to create or deliberately distribute ICT or communications systems “malware”, including viruses, worms, etc.

- to record or monitor telephone or email communications without the express approval of the Governing Body (or the Chair of Governors). In no case will such recording or monitoring be permitted unless it has been established for that such action is in full compliance with all relevant legislation and regulations (see Appendix 1, Regulation of Investigatory Powers Act 2000.

- to enable or assist others to breach the Governors’ expectations as set out in this policy

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

- for participation in “chain” e-mail correspondence (including forwarding hoax virus warnings)

- in pursuance of personal business or financial interests, or political activities (excluding the legitimate activities of recognised trade unions)

- to access ICT facilities by using another person’s password, or to post anonymous messages or forge e-mail messages using another person's identity

Note: The above restrictions apply to the use of phones, e-mails, text messaging, internet chatrooms, blogs, and personal websites (including personal entries on Facebook etc).

The use of own/personal equipment on school property/grounds, or whilst on school business, will be subject to the same restrictions shown elsewhere in this policy relating to the schools ICT equipment and may amount to gross misconduct and could result in dismissal.

Appendix 1

Regulation of Investigatory Powers Act 2000

Ancillary to their provision ICT facilities the Governing Body asserts the employer's right to monitor and inspect the use by staff of any computer (including e-mails) or telephonic communications systems and will do so where there are grounds for suspecting that such facilities are being, or may have been, misused.

In the event of offensive material being found on a school computer which may have been placed there by a member of staff, remove the computer from use and put it in a secure place and seek immediate advice from your HR Business Partner

Appendix 2
Legal issues relevant to the use of ICT and communications equipment

Computer Misuse Act 1990
This was introduced as a means of prosecuting individuals who commit some form of computer crime. Hacking, eavesdropping, deliberate virus attacks are covered. Unauthorised access to a computer is the most likely offence within the Council. Only use machines/systems which you are authorised to use.

Data Protection Act 1998
Individuals have rights about personal data recorded on computer and in manual files. Don't put personal data in the subject line of emails; be careful about including it in the body of the text. An individual can request access to his personal data and this includes email. There are regulations about direct marketing via email.

Copyright, Design & Patents Act 1988
It is an offence to copy software without the author's permission. Downloading application software without permission or forwarding programs in attachments may put you in breach of this act. Some Internet sites will not let you copy material you find there Take care.

The Defamation Act 1996
Facts concerning individuals or organisations must be accurate and verifiable views or opinions must not portray their subjects in a way that could damage their reputation. This applies to internal as well as external email. Organisations in the UK have lost court cases where internal email systems were used to defame other organisations and heavy fines were imposed.

Sex Discrimination Act 1975
Race Relations Act 1976
Disability Discrimination Act 1995

Protection from Harassment Act 1997
Accessing or distributing material which may cause offence to individuals or damage the Council's reputation may lead to a prosecution under these Acts. The fact that it is electronic does not prevent action.

Human Rights Act 1998
The present Government's commitment to incorporating the European Convention on Human Rights into domestic law has led to the introduction of the Human Rights Act 1998. Under this Act a UK citizen can assert their Convention rights through the national courts without having to take their cases to the European Court of Human Rights.

Obscene Publications Act 1959
All computer material is subject to the conditions of this Act, under which it is a criminal offence to publish an article whose effect, taken as a whole, would tend to deprave and corrupt those likely to read, see or hear it.

'Publish' has a wide meaning and is defined as including distributing, circulating, selling, giving, lending, offering for sale or for lease. It seems clear that material posted to a newsgroup or published on a World Wide Web page falls within the legal definition of publishing and is therefore covered by the Act. The publisher would appear to be the originator or poster of the item. The Council is the originator of the Bradford Internet & Intranet sites, or the Governing Body in the case of Voluntary Aided and Foundation schools.

Telecommunications Act 1984
The transmission of an obscene or indecent image from one computer to another via a 'public telecommunications system' is an offence under section 43 of this Act. For traditional mail, the same sort of offence is created under the Post Office Act 1953.

Protection of Children Act 1978
Criminal Justice Act 1988
These Acts make it a criminal offence to distribute or possess scanned, digital or computer-generated facsimile photographs of a child under 16 that are indecent.

Appendix 3

PART 1: to be retained by staff member

This declaration refers to the Governing Body's Policy and Guidance on the use the school's ICT and Communications Systems and the Policy on the use of Social Networking Sites and confirms that you have been provided with copies and that you have agreed to follow them.

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 the guidance on the use of social networking sites and sign the following declaration.

Declaration

You should sign two copies of this document; this copy to be retained by you. The second copy (below) is to be detached and placed your personal file.

I confirm that I have been provided with a copy of the school's Policy on the use of the school's ICT and Communications systems and the Policy on the use of Social Networking Sites. I confirm that I am aware that all my electronic communications including emails and website searches may be monitored by the school and that this applies even if I am working from home on school equipment or networks.

Signed: ..... Name: ..... Date:……

✂----------

PART 2: to be detached and placed on the employee's file

This declaration refers to the Governing Body's Policy and Guidance on the use the school's ICT and Communications Systems and the Policy on the use of Social Networking Sites and confirms that you have been provided with copies and that you have agreed to follow them.

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 the guidance on the use of social networking sites and sign the following declaration.

Declaration

You should sign two copies of this document; this copy to be retained by you. The second copy (below) is to be detached and placed your personal file.

I confirm that I have been provided with a copy of the school's Policy on the use of the school's ICT and Communications systems and the Policy on the use of Social Networking Sites. I confirm that I am aware that all my electronic communications including emails and website searches may be monitored by the school and that this applies even if I am working from home on school equipment or networks.

Signed: ..... Name: ..... Date: ……