

USING E-MAIL AND INTERNET FACILITIES AT SCHOOL: A COMMON SENSE APPROACH

A BRIEFING BY THE NATIONAL UNION OF TEACHERS

CONTENTS

1. Introduction
2. The Internet and the Law
3. An Internet Policy
4. Technical Solutions
5. Education and Training
6. Common Sense Guidelines
7. Workload Issues
8. Access to the Internet and E-mail for Trade Union Representatives
9. References and Resources

1. INTRODUCTION

The opportunities for teachers and pupils to use ICT skills to benefit them in all aspects of school life and beyond are increasing daily. The potential of the internet to enhance teaching and learning is enormous. The expanding use of school internet and e-mail facilities, however, has led to increasing concern by teachers and head teachers about ways to ensure responsible and safe use of this developing communications medium.

Extensive use of Information & Communications Technology (ICT) in schools raises organisational and managerial problems. There is also the potential for misuse of the technology. In recent years, this has included pupils gaining unauthorised access to computer files, the unauthorised deletion of pupils' work on school networks and teachers being accused of misuse or improper use of school facilities.

There are educational, managerial and technical solutions which can help to minimise the risk of the inappropriate use of the internet and e-mail. This NUT guidance is designed to highlight, and raise NUT members' awareness of, some of the key issues which need to be considered when using school equipment to access the internet and e-mail. This is particularly important given schools can reserve the right to monitor use of these systems.

This NUT guidance has been prepared for all schools, although it is recognised that the issues for schools in the primary sector are likely to be different from those in secondary or special schools. Each school will need to decide the measures it needs to take to prevent inappropriate use of the internet and e-mail and to develop responsible use of the technology.

2. THE INTERNET AND THE LAW

Aspects of existing legislation are relevant to the use of the internet and legal precedents are developing in the courts. In many cases, laws relating to copyright, libel, or

incitement to racial hatred apply to the use of the internet as they would for other forms of communication. Child protection legislation applies as do relevant laws on obscenity and indecency. Criminal charges can result from misuse of the internet and teachers have a duty to provide protection for the pupils in their care.

Copyright and the Internet

World Wide Web pages are subject to copyright law. Furthermore, each page may contain several different copyrights if it contains text, music, graphics and so on. Copying from the internet starts when a user starts browsing since copies are made onto the computer's RAM. This copy is likely to be construed as a legal copy implicitly licensed by the copyright owner so long as the copyright owner agreed that it could go on the Web in the first place. However, it should not be assumed that any subsequent copying (such as print-out or copy-and-paste) is legal and users should look on the site for any copyright statement and seek permission from the copyright owner(s) if permission is not granted automatically.

Electronic Copying

Electronic use and copying are not considered to be the same as photocopying. Consequently, it is not legal to undertake activities such as scanning text or images from a paper original into a computer or posting material from the Web or a student's work onto the school intranet without the express permission of the copyright holder or a digitisation licence. A school which has a CLA photocopying licence is not authorised for any digital use or digital storage.

Digitisation Licences

The CLA digitalisation licence permits licensees to digitise textual extracts from certain books and periodicals and to make them available to students and staff over a network. However, at present, the licence does not authorise digitalisation of any artistic works, such as illustrations, diagrams or photographs and permission should be sought from the copyright holder.

The Computer Misuse Act 1990

Legislation was introduced to recognise three key offences as explained below.

- Unauthorised access to computer material, for example, finding or guessing someone's password, then using that to get into a computer system and have a look at the data it contains. This is an offence even if no damage is done, and no files deleted or changed. The very act of accessing materials without authorisation is illegal. This offence carries a penalty of imprisonment up to six months and/or a fine.
- Unauthorised access with intent to commit or facilitate commission of further offences. This builds on the previous offence. It includes guessing or stealing a password, and using that to access material or services without the consent of the owner. For this offence the penalty is up to five years' imprisonment and/or a fine.

- Unauthorised modification of computer material. This could include deleting files, changing the desktop set-up or introducing viruses with the intent to impair the operation of a computer, or access to programs and data. The word 'intent' means it has to be done deliberately, rather than someone deleting files by mistake. This offence carries a penalty of up to five years and/or a fine.

Schools should be aware of the provisions of the Act, and promote responsible behaviours by users through its policies. Schools should also be aware of the provisions of the Act if making facilities available to the wider community outside of school hours, and should develop guidelines accordingly.

Parents will expect schools to promote high standards in relation to the use of computers and the internet, whether or not the material being accessed is necessarily illegal. They will expect schools to develop the same levels of responsibility in pupils in this area as in any other. Schools should take all reasonable precautions with regard to internet access and have strategies to promote responsible use, both within and outside the school.

The Data Protection Act 1998 and Human Rights Act 1998 also have implications for the use of e-mail and internet facilities in schools by placing limits upon the ability of employers routinely to investigate and monitor use of these facilities by teachers. This area is considered in the section "Monitoring the Use of E-mail and Internet".

3. A SCHOOL POLICY ON E-MAIL AND INTERNET USE

The NUT believes it prudent for all schools to have in place a written Policy on E-mail and Internet Access. The policy needs to balance the desirability of fully exploiting the vast educational potential of internet resources for learning and communication with safeguards against the risks and unacceptable activity.. It is important that the policy is reviewed and updated at regular intervals, to ensure that it continues to meet the requirements of the school and any emerging uses of technology. Some schools have chosen to integrate their internet safety policy with other school policies such as child protection, health and safety and anti-bullying. The policy should be clearly understood by staff and pupils alike and communicated to parents.

Any policy to encourage responsible use of e-mail and the internet should:

- specify reasonable limitations on use by staff and pupils and procedures for access authorisation;
- introduce protocols for use inside and outside lessons;
- identify unsuitable sites or materials to which access is unacceptable or prohibited;
- suggest safeguards to prevent personal information being inappropriately accessed;
- provide details of filtering systems, and monitoring carried out by the school;
- set out procedures to avoid virus contamination;

- provide guidance on respect for copyright or breaches of intellectual property;
- establish e-mail etiquette;
- set out a strategy or policy for what to do if an incident or violation occurs;
- describe disciplinary procedures or sanctions which may be applied in the event of misuse;
- identify individual roles and responsibilities.

Guidance on the Data Protection Act 1998 recommends that all employers should give consideration to the establishment of such a policy.

There may be several elements to a schools' acceptable use policy.

- Main policy document: a full and comprehensive policy document which should outline the basis for all aspects of acceptable use of ICT within the school.
- Summary for pupils and parents, setting out the ground rules for safe and responsible ICT use by pupils in school and written in a way that is appropriate for the age of the pupils, and is easily understandable.
- Checklist: a single page checklist may be useful to post next to all ICT facilities to remind users of the key elements of the acceptable use policy.

Where there is no written policy, NUT school representatives should press for the development of a policy as quickly as possible. The policy should be based on consultation and discussion with all staff. The existence of a policy will provide guidance and safeguards for teachers, pupils and parents. It will be appropriate to take the policy into account in any disciplinary proceedings involving employees.

The resources and references section of this guidance provides further information on internet policies.

4. TECHNICAL SOLUTIONS

It is recommended that schools also install appropriate software to help prevent unsuitable sites being accessed. Technical solutions to social issues cannot be expected to be fully effective by themselves, but they should form an important part of the school's approach to protecting both staff and pupils.

- 'Firewalls' protect computer networks and their contents from malicious users and accidental damage, caused either by users from within or outside an organisation. A firewall, for example, could prevent confidential information about pupils being corrupted or seen by unauthorised users. Alternatively it could block access to unsuitable websites. They are generally unable to protect against damage caused by computer viruses.
- Filtering systems prevent or block users' access to unsuitable material. Many will also provide facilities to filter incoming and outgoing e-mail. When the filtering system is turned on, users cannot open or link sites that the filtering system recognises as unsuitable. Although a useful tool, filtering systems are not

foolproof. They should not replace vigilance or simple commonsense from network administrators, teachers or parents.

- Walled gardens are services which offer subscribers access to collections of pre-selected websites. Walled gardens offer the highest form of control and protection against access to inappropriate material. There are a number of commercial internet service providers (ISPs) and local education authorities who offer this service to schools. Some ISPs undertake all the selection and vetting of sites, while others allow subscribers to supplement or amend the 'allow' list themselves. Several ISPs are also now offering subscribers the ability to create an additional 'deny' list of sites that they wish to have blocked.

E-mail and search engines generally fall outside the protection of a walled garden and so potentially allow access to inappropriate sites. Several ISPs are considering this issue and it is probable that context-sensitive filtering will become more widespread.

- A virus is a piece of programming code usually disguised as something else that causes some unexpected and usually undesirable event, and is often designed so that it is automatically spread to other computer users, for example as an e-mail attachment, as a file download, or on floppy disk or CD. All schools should invest in efficient and up-to-date virus protection software, which is a program that searches for any known or potential viruses and either deletes or repairs the problem. Some anti-virus software is free of charge and can be downloaded directly via the web, while others are available for purchase. Anti-virus software offers different levels of protection and the level of protection required by the school should be a key consideration when implementing.

In addition, both staff and pupils, however, should be made aware of the sensible measures they should take to prevent viruses. Schools may wish to use the following simple five-stage test to avoid viruses.

- The Know test: Is the e-mail from someone that you know?
- The Received test: Have you received e-mail from this sender before?
- The Expect test: Were you expecting e-mail with an attachment from this sender?
- The Sense test: Does e-mail from the sender with the contents as described in the subject line and the name of the attachment(s) make sense?
- The Virus test: Does this e-mail contain a virus? Always check it using anti virus software.

5. EDUCATION AND TRAINING

Pupils

New technologies are penetrating into every area of everyday life, where access is likely to be less controlled than it is at school. Home access to the internet and related services such as e-mail, instant messaging and chat services are now common. Children therefore need to be taught to use these new technologies safely and responsibly both within school and outside.

Younger pupils cannot be relied upon to foresee every possible danger. Faced with suspect material, even the most responsible children may not have the experience or

maturity to make informed judgements, therefore the school will need to regulate internet access.

For infants and some juniors, schools may control internet access by an adult working with a small group of pupils. An approach may be taken with older primary and secondary pupils, whereby the school establishes a code of conduct. Both types of approach, education and regulation, may be appropriate depending on age and maturity of the pupils. Each school will need to strike the right balance in writing its internet access policy.

Many of the risks of pupils using the internet and related technologies can be further minimised by taking a commonsense approach, for example:

- siting computers in public places where everyone can see what is on the screen;
- monitoring on-line time and being aware of excessive hours spent on the internet;
- warning young people that there are some unsuitable sites on the internet and that people may try to contact them in an inappropriate way and discussing the issues involved; and
- setting up a reporting system so that students know what to do if they find upsetting material.

Pupils' use of the internet may be greater at home than in school. The NUT believes that the school's internet policy should be communicated to parents, so that the same protection can be extended into the home environment.

Wherever pupils interact with the public by telephone, e-mail, or web site, particular care is required to ensure the communication is appropriate. Pupils need to follow sensible rules for personal safety, for instance, never giving full name, a home address or telephone number.

Access needs to be planned to prevent the most enthusiastic or assertive pupils dominating use. An explicit reference to equality of ICT access in the school development plan will help remind teachers that equality of access in the classroom needs to be monitored.

School Staff

It is vital that schools allow opportunities for the professional development of all staff in information and communication technologies. Staff awareness of the issues relating to the use of ICT and understanding of the school's strategies is also important. Time will be required for teachers to integrate ICT into the curriculum, in particular, revision of the teaching of study skills.

In order to support the development of teachers' ICT skills, schools should encourage home access to ICT and particularly the internet. As ICT is increasingly seen as an essential tool for teaching, the NUT believes that current Government ICT initiatives should be extended and that all teachers should be provided with a laptop, which can be used both in the classroom and elsewhere, and to high quality continuing professional development which will meet the particular needs of the individual teacher. Such a view

is supported by evidence from OFSTED, which found that “*personal access for teachers to a computer for the purposes of preparation and planning is one of the strongest influences on the success of both ICT training and subsequent classroom use*”

Health and Safety

Both pupils and staff should be trained on safe use of ICT facilities and should be provided with appropriate information and equipment to avoid risks such as Repetitive Strain Injury (RSI) or back problems arising from inappropriate use. NUT guidance in this area is available in the NUT health and safety briefing, “Working with Computers”, available in the health and safety section of the NUT website at <http://www.teachers.org.uk/story.php?id=1545>

6. COMMON SENSE GUIDELINES

Using Facilities for Professional Purposes

It is reasonable for the principles described below to form part of school policies.

- Pornographic sites should not be accessed under any circumstances. Any teacher who uses school internet facilities to download pornographic materials is likely to be judged as committing an act of gross misconduct.
- Access to other offensive or inappropriate sites should also be avoided. There may be circumstances where access to such material is necessary to inform teaching and learning. In such cases, prior written permission to use such material should be obtained.
- It would be inadvisable for teachers to access chat rooms, for either professional or personal purposes, without first obtaining written authorisation to do so.
- Downloading software and other data from the internet onto the school network or hard disk should be undertaken with caution in order to protect against viruses. If in doubt, advice should be sought from the ICT co-ordinator or network manager.
- Great care should be taken to ensure personal access passwords remain confidential to avoid misuse by others.
- The actions of all users of the internet are durable and can be traced. Internet users leave a record in the browser of everything they have looked at and of all e-mails sent or received. If inappropriate material is inadvertently accessed or received by pupils or staff, this must be reported immediately to the person with overall responsibility.

Personal Use of Facilities

A common sense approach should apply to the use of the internet for personal purposes by teachers.

Facilities provided by employers are provided for work-related activities. This applies equally to school internet and e-mail facilities, whether within the school building or outside it. Even where teachers use such facilities during lunch-breaks or outside working hours, the equipment still belongs to the employer and use without permission creates the possibility of disciplinary action on the basis of unauthorised use.

Reasonable employers will permit school staff to make limited personal use of e-mail and internet facilities provided that this does not interfere with the performance of their duties. This includes access for NUT's members to the NUT's website. This is particularly the case where limited personal phone calls are already permitted or where personal use of such facilities would limit costs to the employer in terms of time or money. It is reasonable, however, for such use to be restricted to the beginning or end of the school day or to lunchtimes. Teachers are advised to check their employer's expectations regarding personal use of facilities if this is not explicit in the school policy.

Use of e-mail and internet facilities should therefore be included in school policies. If a situation arises where teachers need to use the internet for a reason which is not specified in the policy, then they should obtain prior authority in writing from whoever has overall responsibility.

It would, however, be advisable for NUT members to clarify the employer's position regarding personal e-mail and internet use and to avoid using the school e-mail facility to send excessive numbers of personal e-mails.

Monitoring the Use of E-mail and the Internet

Government guidance¹ issued under the Data Protection Act, recommends good practice to be adopted when organisations wish to monitor the activities of their workers, including their use of internet and e-mail facilities at work.

The Data Protection Act does not prevent an employer from monitoring workers but requires that such monitoring is conducted in a manner consistent with the Act. Also relevant, especially to public sector employers, is the Human Rights Act which provides a right to respect for private and family life and for correspondence.

The Government's guidance sets out certain core principles which should govern employers' approach to monitoring. The first is that it is usually regarded as intrusive to monitor workers. The second is that workers have legitimate expectations to keep their personal lives private and to a degree of privacy in the work environment. The third is that employers wishing to monitor their workers must be clear about the purpose of monitoring and satisfied that it is justified by real benefits that will be delivered. Alternatives to monitoring must be considered. Relevant issues for consideration include whether the monitoring will be oppressive or demeaning; and the impact it will have on the relationship of mutual trust and confidence that should exist between employer and employees.

Compliance with the Code in schools can be achieved by establishing in the school policy that investigations will be undertaken only where complaints have been made about a particular member of staff, or where a particular member of staff is arousing

¹ Part 3 of the Employment Practices Data Protection Code, published by the Office of the Information Commissioner under Section 51 of the Data Protection Act

suspicion, rather than subject all staff to monitoring. Effective communication to staff of the school policy on the use of internet and e-mail facilities should, in any case, render monitoring unnecessary.

7. WORKLOAD ISSUES AND AVOIDANCE OF BUREAUCRATIC BURDENS

The immediacy of e-mail can lead to expectations of instant action, or response, to messages sent. There is also likely to be a degree of pressure during the introduction of new facilities or practices, particularly for those that are unfamiliar with the new equipment or systems. Increased pressure or workload as a result of e-mail communications should be addressed in the context of the NUT guidance on 'Reducing the Bureaucratic Burden on Teachers'. This guidance gives clear advice on how to respond to unreasonable demands relating to the use of ICT and is available on the NUT website www.teachers.org.uk

The ongoing initiatives to relieve teachers of the burden of administrative and clerical tasks and the NUT's campaigns on this area mean that teachers should consider carefully whether any aspects of non-teaching work involving use of the internet could more appropriately be carried out by a member of the support staff. Basic internet searches, ordering of items and downloading of documents are examples of tasks that do not necessarily require the expertise of a teacher and should be undertaken by support staff members. In depth research, however, would in most cases remain within the remit of the teacher.

The Union's guidance '*Advice, Guidance, Protection: School Workforce Reform and New Teachers' Regulations*' sets out the "key questions approach", which should be used by members to ensure that they maintain control on exercising their professional skills and judgement in relation to administrative and clerical tasks whilst, at the same time, being free from administrative and clerical burdens. This guidance is available on the NUT website www.teachers.org.uk

Other issues

The same advice applies to e-mail harassment as any other form of workplace bullying. Any NUT member who feels harassed by the receipt of e-mail should contact their NUT regional office or in Wales the NUT Wales Office, NUT Cymru for further advice.

Insurance

Teachers need to know what responsibilities they have, if any, for insurance. Where equipment is owned by an organisation, but in the long-term possession of the employee, home insurance companies have been known to be difficult about meeting insurance claims. Existing LEA and school insurance policies should be extended to cover the use of school computer equipment outside school premises, such as laptop computers used by teachers at home. This should include transit between school and a teacher's home.

8. ACCESS TO INTERNET AND E-MAIL FOR UNION REPRESENTATIVES

The "Burgundy Book" national agreement on facilities for trade union representatives recommends that certain facilities should be made available to trade union representatives including NUT school representatives as well as NUT local officers to enable them to discharge their functions. These include use of telephone, with payment for outgoing calls, and use of typing, duplicating and photocopying equipment, provided that this does not interfere with the work of the school and on the basis of repayment by the organisation for the materials used.

The NUT believes that, in the light of advances in technology, access to e-mail and internet facilities should also be permitted, particularly since such use would be unlikely to result in any increase in costs for the school concerned. Trade union representatives' use of internet and e-mail facilities should, of course, be in accordance with the school's policy on the use of such facilities.

Acknowledgements

Certain publications were very helpful in terms of drafting this advice. In particular the NUT made reference to the National Grid for Learning (NGfL) publication "Superhighway Safety: Using Technology Safely in Schools". The model internet access codes of conduct for staff and pupils is based on advice to schools developed by Kent County Council.

9. RESOURCES AND REFERENCES

Listed below are a selection of organisations that provide useful information relating to establishing an internet Access Policy, technical solutions etc.

Association of Co-ordinators and Teachers of IT (ACITT)

<http://acitt.digitalbrain.com/acitt/index.htm>

Wide range of information on educational and administrative ICT issues

BECTA

www.becta.org.uk

Advice and guidance on computer misuse

British Computer Society

<http://www1.bcs.org.uk/link.asp?sectionid=301>

Advice and guidance for headteachers, governors, and ICT co-ordinators on writing school ICT acceptable use policies.

Childnet

<http://www.childnet-int.org/>

Advice to children, parents and teachers about the safe use of the internet.

The Computer Emergency Response Team

<http://www.cert.org/>

US site providing in depth, up-to-date information on protecting against viruses

Computer Misuse Act 1990

http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

The full text of the Act

DfES Virtual Teacher Centre

www.vtc.ngfl.gov.uk/vtc/schoolman/policies.html

Government information on developing policies for ICT usage in schools

Information Commissioner on the Data Protection Act

www.dataprotection.gov.uk

Employment Practices Data Protection Code – Part 3: Monitoring at Work

Intellectual Property Group

http://www.intellectual-property.gov.uk/std/faq/copyright/material_internet.htm

A Government site providing specific information about intellectual property on the internet

Internet Proficiency Scheme

http://www.gridclub.com/grown_ups/cont_ict_cyb.shtml

A Key Stage 2 resource developed by BECTA. A free teachers' pack can be obtained by contacting the DfES publication order line(Phone: 0845 60 222 60 Fax: 0845 60 333 60, Minicom: 0845 60 555 60, Email: dfes@prolog.uk.com)

Internet Watch Foundation

www.internetwatch.org.uk

Information on illegal material on the internet. This site also invites people to report inappropriate web sites. Funded by DTI

Kent County Council

<http://www.kented.org.uk/ngfl/policy.html>

Comprehensive information on implementing an internet Access Policy

Laptops for Teachers

www.lft.ngfl.gov.uk

Details on the DfES laptops for teachers initiative

National Association of Advisers for Computers in Education (NAACE)

www.naace.org/

Guidelines on using the internet safely and insurance issues

National Grid For Learning

<http://safety.ngfl.gov.uk/>

Advice on all aspects of Internet safety for schools and LEAs.

Northamptonshire County Council

<http://www.northants-ecl.gov.uk/apps/gen/dtp/hme.asp>

A basic toolkit for headteachers, staff and governors, to help them comply with data protection requirements and related legislation:

Parents Information Network (PIN)

www.pin-parents.com

An introduction to the internet – comprehensive guidelines on using the internet safely