

Medway Grid for Learning

Policies and Guidance



Security and Acceptable Use Policies

(Version 3.10 - 29/07/2002)

1	Security Policy.....	2
1.1	Objective	2
1.2	Approach	2
1.3	Policy for Connection to SEGfL.....	2
1.4	Email system access.....	2
1.5	Local school mail servers	2
1.6	Virus scanning.....	2
2	Internet Access Policy (IAP).....	2
2.1	Model policy available for adaptation	2
2.2	Acceptable use policy – Internet	2
2.3	Acceptable Use Policy – E mail.....	2
2.4	School Web sites.....	2
2.5	References	2
2.6	Useful references for schools.....	2

Introduction

This document is intended to provide general information and guidance related to connecting school LANs to the broadband Grid for Learning network, and running school systems and servers effectively to deliver a reliable, high performance service. It also provides specific policies adherence to which is necessary for the smooth and effective running of the whole network.

1 Security Policy

1.1 Objective

This security policy is designed to ensure that the security and integrity of computer systems connected to the Medway Council network, in particular the Education section, is maintained.

1.2 Approach

The connection of schools and LEAs to the Internet brings many benefits. However the careful and thorough implementation of a security policy is required to maintain. Each school is unique and the effective, appropriate and safe use of ICT facilities depends on many factors. It is therefore important that each school devises their own policy for computer use, and this document is intended to provide a sound framework and save schools work.

1.3 Policy for Connection to SEGfL

All staff must understand their responsibility for the integrity and security of the Wide Area Network service and that a breach of security could result in disconnection until the cause of the breach is resolved. Schools wishing to connect to the Medway SEGfL broadband network must undertake to implement the following rules.

- An ICT Security Manager shall be appointed, who will be a senior member of staff.
- The school must have a current Internet Access Policy covering the use of e-mail, Web, publishing and other applications.
- All connections to external networks, including other dial-up access to the Internet, must be removed. Remote access facilities for third party support will be provided centrally for approved maintainers. Contact the Network Operations Centre on 01634 332525 if you need this facility set up for one of your suppliers.
- The Sophos anti-virus product, or another approved and current virus checker must be installed on every workstation and server.
- All hardware and software and network connections must be approved by the ICT Security Manager.
- The ICT security manager shall ensure that the requirements of Data Protection Acts, Computer Misuse Act, and other relevant Acts pertaining to I.T. and data storage are observed.
- To ensure users are aware of their responsibilities, the ICT Security Policy should be published and agreement to comply with the policy obtained.
- Any directions given to mitigate the risks and effects of future security threats must be followed promptly. Responsibility for ensuring this shall lie with the ICT Security Manager.

1.4 SEGfL Network Equipment

Under no circumstances should you unplug or reorder the connections to the SEGfL network hardware unless specifically directed to do so by Medway Council network support staff. This equipment generally includes an APC uninterruptible power supply (UPS), a Cisco 1700, 2600 or 3600 series router, and in the case of some schools, a Cisco Catalyst 3524 switch. Also you should not switch off the equipment, or remove power to it, except in the case of an emergency, without first informing the Network Operations Centre on 01634 332525.

All hardware is monitored 24 hours per day and failure to observe the requirements above will result in unnecessary call-outs for support engineers.

1.5 Email system access

The Email system is available from the Internet. This feature has been made available due to the evident usefulness of access from the Internet, however caution should be exercised as it is not inconceivable that a user's password could be retrieved from a PC used to connect to the service.

1.6 Local school mail servers

The IMail email system is scanned by the Sophos Server Anti-virus product and updated regularly. If a school runs a local email server this server must also have the Sophos anti-virus product, or another approved and current virus checker installed.

1.7 Virus scanning

Virus scanning software is essential to protect all machines against the threat of virus infection, mainly from floppy disks or from CDROMs and internal emails which may be sent from another infected machine. The Sophos anti-virus product is available at no additional charge as part of the SEGfL service in Medway.

The homepage for this service can be found on the support site at <http://support.medway.org.uk/support/faq/sophos/sophosindex.asp> - this is intended for use by ICT technicians and coordinators and requires the 'ftp' username and password to access it. The page shown allows the full product to be downloaded as well as signature updates which are needed to ensure the product continues to provide protection against new viruses.

2 Internet Access Policy (IAP)

The statutory curriculum expects pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan for and make use of communications technology, for example, web-based resources and e-mail. Access to life-long learning and employment increasingly requires computer and communications use and pupils need to develop ICT life skills in their use. Home and social Internet use is expanding and it is becoming an important part of learning and communication during leisure time. This brings pupils into contact with a wider range of information, the scope and nature of which may - or may not - be appropriate for the pupil.

The Medway IAP is a template which helps schools form and implement their own policy. It takes the form of a series of questions with a range of statements that schools can use to form a policy suited to their particular needs and ethos.

Amongst many suggested statements, the following are aspects of the Internet access policy considered essential for Medway schools:

- *In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will supervise pupils and take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear on a terminal.*
- *The school will work in partnership with parents, the LEA, to ensure systems to protect pupils are reviewed and improved for both home and school use;*
- *Pupils will be informed that their use of the Internet will be supervised and monitored appropriately;*

2.1 Model policy available for adaptation

This examples can be used for adaptation when writing school policies:

<http://atschool.eduweb.co.uk/acitt/aup.html>

Detailed below are some of the key areas which should be included in policies.

2.2 Acceptable use policy – Internet

- The policy should be signed by students detailing how the Internet will be used in school.
- There should be a balance between the use of vast educational resources and safeguards.
- Potential users should be taught to develop their information literacy skills and to be able to recognise the bias inherent in sites.
- There should be a code of conduct for Internet use.
- A range of supervision and monitoring strategies should be in place.
- There should be a purpose to the use, can you answer the question; “ Why are we using the Internet?”
- Users should be evaluating Internet content.
- Ensure risk assessment is in place.
- **There should be sanctions for misuse, including bullying, misuse of passwords, libel etc.**
- There should be a process for the reporting of unsuitable sites.
- There should be a complaints procedure for both parents and users.
- There should be an understanding of the need for monitoring users activity on the Internet.

2.3 Acceptable Use Policy – E mail

- Class/ group/ pupil email addresses as appropriate.
- A code of conduct for use
- Encouragement of parents to follow and support guidelines set by school.
- Children should be taught effective communication skills both written skills and personal safety when using email.
- Recognizing all incoming and outgoing email as public property to reduce inappropriate use.
- There should be a range of supervision and monitoring strategies.
- There should be a clear purpose for the use of email.
- Policy and practice should be monitored, reviewed and evaluated regularly.
- To achieve best practice in policy writing it should be written by the team which is implementing, monitoring and reviewing the procedures.

2.4 School Web sites

School web sites are becoming a key factor in the school improvement strategy.

Guidance for protocols may be found at:

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

2.5 References

Useful references for parents

National Action for children www.nchafc.org.uk/internet

Internet Watch Foundation www.iwf.org.uk

Parents Information Network <http://www.pin.org.uk>

2.6 Useful references for schools

Associations of Coordinators of IT <http://atschool.eduweb.co.uk/acitt/aup.html>

BECTa www.becta.org.uk/technology

British Computer Society www.bcs.org.uk/iap.html

DfEE Superhighway Safety <http://safety.ngfl.gov.uk>

Internet Watch Foundation www.iwf.org.uk

Kent NGfL Initiative www.kented.org.uk/ngfl

Scottish Education Department www.scotland.gov.uk/clickthinking

Copyright www.templetons.com/brad/copymyths.html