

Subject:

INTERNET SAFETY

Circular Number:

2011/22

Date of Issue:

27 September 2011

Target Audience:

- Principals and Boards of Governors of all grant-aided schools;
- Education and Library Boards;
- Council for Catholic Maintained Schools;
- Council for the Curriculum, Examinations and Assessment;
- Comhairle na Gaelscolaíochta;
- Northern Ireland Council for Integrated Education; and
- Teachers' Unions.

Summary of Contents:

This Circular represents an addendum to Circular 2007/1, which provided guidance on the safe use of the internet and digital technologies in schools. It includes advice and guidance on arrangements for preventing the accessing of inappropriate material on the Internet, the use of materials from blocked sites, and the provision of information to parents.

Enquiries:

Any enquiries about the contents of this Circular should be addressed to:

Curriculum Support Team
Department of Education
Rathgael House
43 Balloo Road
Rathgill
BANGOR
BT19 7PR

Governor Awareness:

Essential

Status of Contents:

Advice
guidance for schools

Related Documents:

DE Circular 2007/1

Superseded Documents:

None

Expiry Date:

Not applicable

DE Website:

<http://www.deni.gov.uk>

Tel: 02891 279753

Fax: 02891 279100

E-mail:

curriculum.supportteam@deni.gov.uk

Background

1. The purpose of this Circular is to provide guidance about: -
 - C2k filtering of internet access, and the accessing and reporting of inappropriate material;
 - security considerations within a non-C2k system;
 - classroom use of materials and resources from blocked websites; and
 - informing parents about blocked websites.

Filtering within the C2k System

2. C2k provides an effective filtering system, as a result of which the following categories of websites are not, by default, available to schools: -
 - **adult**: content containing sexually explicit images, video or text, the depiction of actual or realistic sexual activity;
 - **violence**: content containing graphically violent images, video or text;
 - **hate material**: content which promotes violence or attack on individuals or institutions on the basis of religious, racial or gender grounds;
 - **illegal drug taking and the promotion of illegal drug use**: content relating to the use or promotion of illegal drugs or misuse of prescription drugs;
 - **criminal skill/activity**: content relating to the promotion of criminal and other activities;
 - **gambling**: content relating to the use of online gambling websites or information relating to the promotion of gambling and gambling advice.
3. C2k defines three types of access:
 - **GREEN** – accessible to all users in schools;
 - **AMBER** – accessible to schools' selected groups of users (can be changed by the C2K School Manager within Post-primary and Special schools only);
 - **RED** – not accessible to any user.
4. A filtering service, no matter how thorough, can never be comprehensive and it is essential both that schools have a clearly understood policy on acceptable use for all users and that adequate supervision is maintained. If at any time school staff or pupils find themselves able to access from within the C2k system internet sites which they think should be blocked, they should advise the school Principal (or, in his absence, his immediate deputy). The Principal should then report the matter to **the C2k Helpdesk** which will implement agreed procedures for handling such issues. Depending on the nature of the issue, these procedures may require C2k to report to the Department. All actions should be taken immediately.

Security considerations within a non-C2k System

5. If a school sets up its own school network, separate from the C2k managed service, with its own internet connection and Internet Service Provider (ISP), it is

the school's responsibility to ensure that the filtering system provided is of an appropriate standard to ensure the safety of its pupils. Whether a school has an agreement with its ISP for a filtering system, or has the expertise to install and maintain its own filtering system, it is vital that it has a filtering policy in place. In drawing up such a policy, a school should ensure that the following are taken into account (this list is not exhaustive).

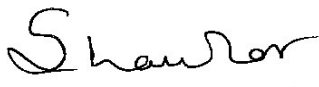
6. The Board of Governors should be informed before non-C2k-based internet access is established, and should be made aware of the implications of such a course of action. Governors should satisfy themselves that the policy conforms fully to all relevant guidance, including that relating to internet safety (including DE Circular 2007/1 on internet safety) and safeguarding.
7. Effective firewalls, filtering and monitoring software mechanisms must be in place. Schools should regularly review their filtering and blocking policies and procedures. Information on the security issues which need to be considered when making use of non-C2k computers is attached as an Annex to this Circular.
8. Procedures must be in place to ensure continuity of expertise so that the system can survive staff turnover.
 - Criteria for blocking and unblocking sites should be clearly communicated to all staff members and parents.
 - Reporting lines from the school to the named ISP, the Board of Governors and parents, and, where necessary, the police, must be clearly set out and understood.
 - Where an incident is likely to involve media interest, the Department should be informed.

Classroom use of materials and resources from blocked websites

9. Where a school has retained printed materials downloaded from websites which have subsequently been blocked by C2k or the school, it must decide (with the approval of its Board of Governors where necessary) whether it wishes to continue to use those resources for teaching and learning. In making that decision, a school should consider the wider implications - for example, the continuing use of otherwise unobjectionable materials from a blocked site could be interpreted as endorsing an undesirable organisation or person associated with the blocking. Where parents are to be informed of the blocking of access, they should also be advised of any consequences for a pupil of bringing resources associated with the site into school.
10. A school's paramount consideration should always be the safety of pupils and staff.

Informing Parents

11. The Department's Circular 2007/1 on Internet Safety provides advice and guidance on drawing up policies for the safe and acceptable use of the internet and digital technologies. That Circular notes that while there is no legal requirement on a school to keep parents informed, it is nonetheless a responsible step for it to take. It is, for example, a matter of good practice to provide parents with a copy of, or access to, a school's internet safety policy.
12. Schools' internet safety policies should include procedures for ensuring that any resources or materials downloaded by teachers, pupils or parents from outside C2k (or the school's own filtered network) are suitable for use in the classroom.
13. Schools should make their own judgments on when to inform parents that access to a website has been blocked, or that the school itself does not feel that an accessible resource is suitable for its pupils. Schools should consider principally the importance and urgency of any given issue, and its relevance to parents. For example, there can be no expectation that routine or merely technical issues should be brought to parents' attention.



SHARON LAWLOR
Head of Curriculum Support Team

Issues to be considered by schools accessing the Internet outside the C2k service

Introduction

A school's policies in relation to internet safety and the use of any systems outside the C2k service should be approved by the school's Board of Governors, who should take account of all relevant guidance, including that relating to internet safety and safeguarding.

1. Risks

When a school opts to provide a separate local network with its own internet access, and uses this in parallel with, though distinct from, its C2k network, it needs to be aware of the potential risks such access can pose if comprehensive security measures are not implemented. The risks associated with insecure internet access include:

- i. attacks from hackers which could result in loss or destruction of data, negative impact on system performance and take-over and use of school machines to launch attacks on other systems;
- ii. accessing inappropriate and/or illegal content;
- iii. inappropriate use of social networks, chat rooms, etc.;
- iv. theft of user credentials;
- v. virus attacks.

2. Security

A range of security measures needs to be put in place to secure against such risks. These measures include the following.

- i. **Firewalls**
These enforce security policies which protect the network from unauthorized access to data and services.
- ii. **Intrusion prevention systems**
These monitor and analyse network traffic and detect viruses, hacking tools and suspicious traffic.
- iii. **Content filtering**
This manages, monitors and controls access to internet sites. A range of commercially available filtering packages is available. All operate in a similar way, by checking all sites accessed against a comprehensive database that is regularly updated. Filtering systems may vary in the range of tools they use

and in the granularity (level of detail) of their filtering.

iv. **Email scanning and filtering**

This automatically scans all incoming and outgoing emails for viruses, banned file types and spam.

v. **Secure hosted applications**

These are applications (e.g. a social network, Virtual Learning Environment (VLE), etc.), which may be downloaded from the internet and installed on local servers in a school. They will usually include a range of applications, scripting language, web servers, a user authentication service and an operating system. See paragraph ix below for data security considerations.

vi. **Ongoing vulnerabilities assessment**

This is done to ensure that there is regular testing of all systems against new vulnerabilities to protect against exploitation by hackers.

vii. **User authentication using encryption**

This ensures that user login details cannot be intercepted while in transit over the internet. Encryption such as SSL (Secure Sockets Layer) can be used. Depending on what a school uses its own internet access for, some or all of the above will need to be implemented. Where a school implements a comprehensive system which provides access to a range of services and content, it will also need to ensure that there is continuity in terms of personnel with the knowledge and skills to maintain both the system and the security it requires.

viii. **Content filtering**

Any school that provides internet access for pupils and teachers via an internet connection outside the C2k system will need to provide a content filtering solution. Such solutions come with a set of default settings. However, the school will need to define and implement its own filtering policy and ensure that it is kept under constant review. This is because the direction and growth of Web 2.0 technologies mean that internet sites are no longer simply flat HTML pages. Sites are now immensely complex and it can happen for example, that, while the main part of a site can be considered appropriate, it may contain subsections which will need to be filtered.

ix. **Data security**

Schools are data controllers under the Data Protection Act 1998, and must register their data needs and operations with the Information Commissioner's Office. They must therefore satisfy themselves about the security of school and pupil data, particularly if they choose to use a secure hosted application such as a VLE or social network that holds user data in the "Cloud". (Cloud computing involves the provision of anytime, anywhere access to a range of applications for anyone who has an internet connection.) In terms of data security the crucial factor is that such applications are data repositories that hold the user data in servers that can be located anywhere, with the result that the user does not know where his data is located. Thus, while this type of technology may be of benefit when the data or information is not personal or

sensitive, using Cloud computing applications to host such data requires careful consideration of (inter alia) the terms and conditions of the service provided, privacy arrangements, perpetuity and the portability of data should a school wish to delete or move its data. The school may need to seek legal advice to ensure that its provision conforms to the requirements of the 1998 Act.