Department of Education
www.deni.gov.uk
AN ROINN Oideachais
MÂNNYSTRIE O Lear

INVESTOR IN PEOPLE

Subject:

eSAFETY GUIDANCE

Circular Number:

2013/25

Date of Issue:

6 December 2013

Target Audience:

- Principals and Boards of Governors of all grant-aided Schools;
- Education and Library Boards;
- Council for Catholic Maintained Schools;
- Council for Curriculum, Examinations and Assessment
- Comhairle na Gaelscolaíochta;
- Northern Ireland Council for Integrated Education;
- Governing Bodies Association;
- Teacher Unions; and
- Education and Skills Authority Implementation Team.

Summary of Contents:

This Circular reminds schools about their responsibility to have in place an eSafety policy. It provides guidance on eSafety in the context of the new C2k contract, Education Network (ni) and in relation to non C2k networks.

Enquiries:

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

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

Governor Awareness:
Essential

Status of Contents:
Advice

Related Documents:
Circular 2007/1
Circular 2011/22

Superseded Documents:
Circular 2007/24

Expiry Date:
Not applicable

DE Website:
http://www.deni.gov.uk
Tel: 02891 279936
Fax: 02891 279100
E-mail:
curriculum.supportteam@deni.gov.uk

1. INTRODUCTION

1.1 Through the DE funded C2k Managed Service all schools have access to a core set of technologies to help teachers and pupils with teaching and learning. The roll-out of the new C2k contract, Education Network (ni), commenced in April 2012 and is underway at present. Along with increased broadband, a major enhancement in the new services lies in the ability to accommodate the connection of a range of third-party access devices into the school network. This will allow the school to plan for, and exploit, circumstances where pupils might make use of their own devices to connect to the service anytime, anywhere. Schools will also have the option of opening up to pupils, social media sites they consider contribute to improved teaching and learning. These service improvements bring along with them challenges for schools in relation to their statutory responsibility for ensuring the welfare and safety of both teachers and pupils.

1.2 The purpose of this circular is to remind schools about their responsibility to have in place an eSafety policy and an Acceptable Use Policy (AUP). Section 4 of this circular provides you with information on what should be included in your school's eSafety policy, including advice if any of your staff and pupils are using non C2k Equipment on a legacy network or if they are accessing the Internet through school provided non C2k connections. Section 4 also provides a link to sample AUPs available via the Department's website. Supporting materials and guidance are also available via the C2k Exchange.

2. WHAT IS eSAFETY?

2.1 eSafety is short for electronic safety.

2.2 It highlights the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. eSafety covers not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

2.3 eSafety in the school context:

- is concerned with safeguarding children and young people in the digital world;
- emphasises learning to understand and use new technologies in a positive way;
- is less about restriction and focuses on education about the risks as well as the benefits so that users feel confident online;
- is concerned with supporting pupils to develop safer online behaviours both in and out of school; and

- is concerned with helping pupils recognise unsafe situations and how to respond to risks appropriately.

2.4 The rapidly changing nature of the Internet and new technologies means that eSafety is an ever growing and changing area of interest and concern. The school's eSafety policy must reflect this by keeping abreast of the changes taking place. Schools have a duty of care to enable pupils to use on-line systems safely.

2.5 All schools should have their own eSafety Policy, which must operate in conjunction with other school policies including Behaviour, Child Protection, Anti-Bullying and Acceptable Use. eSafety must be built into the delivery of the curriculum. ICT is a compulsory cross-curricular element of the revised curriculum and schools must ensure acquisition and development by pupils of these skills.

3. NEW C2K CONTRACT

3.1 The new C2k services to be put in place during 2013/2014 have been designed with a clear focus on eSafety. The main eSafety elements that Principals, Senior Management Teams and Governors need to prepare and plan for the introduction of are outlined in the table below.

Internet Filtering	Improved Websense filtering will give schools the flexibility to control and develop their own Internet Filtering Policy. Individual schools may now select to fully delegate management of their filtering policy to a nominated member of staff by signing up to C2k delegated filtering access. This nominated user will receive additional training for this responsibility and can further amend the local filtering policy to the needs and demands of the school. This is in direct response to feedback from schools, who wish to access more internet sites to enhance teaching and learning. However there are a number of agreed locked down sites that can never be overridden by the local school policy.
Meru Wireless	Meru Wi-Fi will provide increased wireless coverage and improved speed. Meru supports multiple devices and school controlled secure guest access and allows schools to plan for and implement a further purchase by the school or/and a 'Bring Your Own Device' policy.
Cloud Storage	Data and information will be stored on the Cloud in the new service and no longer in the school itself. This means it can be securely accessed from any location removing the need to carry data and files on insecure data pens and portable devices.
Personal Devices	Schools will be able to explore the introduction of new internet enabled devices to support teaching and learning.

	These include PCs, laptops, netbooks, tablets and phones. Control of access to the internet is managed by the school and must be enabled for each device.
Granular Controls	Through the new management console, each school C2k Manager will be able to control access to the internet and services to named individuals and groups of users based on their role in the school, their age, courses studied or to support individual needs.

4. ACTIONS FOR SCHOOLS

Review and Amend your School's eSafety Policy

4.1 A school eSafety policy should include sections on:

i. Professional Development for Teachers

Teachers are the first line of defence in eSafety; their observation of behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to illegal activity. Staff should avail of training and support to determine what action is appropriate including when to report an incident of concern to the school Designated Teacher for Child Protection or the member of Senior Management with responsibility for eSafety. Additional support and advice is available from C2k, Social Services or the PSNI if required.

eSafety training is therefore an essential element of staff induction and should be part of an on-going Continuous Professional Development programme. Through a clear and effective eSafety policy, schools can ensure that all reasonable actions are taken and measures put in place to protect all users.

ii. Education of Pupils

The Internet is an integral part of pupils' lives, both inside and outside school. There are ways for pupils to experience the benefits of communicating online with their peers, in relative safety. Child Exploitation and Online Protection (CEOP) resources are a useful teaching tool for all Key Stages looking at Internet safety and can be usefully incorporated into a PDMU/LLW or ICT programme.

See ***www.thinkuknow.co.uk***

Childnet International is a non-profit organisation working to "help make the Internet a great and safe place for pupils". Childnet have produced many materials to support the teaching of eSafety at Key Stage One and Two. They have also produced materials for parents, staff and post primary pupils. Their materials are available to access online or order from ***www.childnet.com.***

iii. Risk Assessments

21st century life presents dangers including violence, racism and exploitation from which pupils need to be reasonably protected. At an appropriate age and maturity they will need to learn to recognise and avoid these risks — to become “Internet-wise” and ultimately good “digital citizens”. Schools need to perform risk assessments on the technologies within their school to ensure that they are fully aware of and can mitigate against the potential risks involved with their use. Pupils need to know how to cope if they come across inappropriate material or situations online. The school risk assessments should inform the teaching and learning, develop best practice and be referenced in the school’s Acceptable Use Policy.

iv. Cyber Bullying

Staff should be aware that pupils may be subject to cyber bullying via electronic methods of communication both in and out of school. This form of bullying should be considered within the schools overall anti -bullying policy and pastoral services as well as the eSafety policy.

Care should be taken when making use of social media for teaching and learning. Each of the social media technologies can offer much to schools and pupils but each brings its own unique issues and concerns. Each social media technology that is to be utilised should be risk assessed in the context of each school situation.

Cyber Bullying can take many different forms and guises including:

- Email – nasty or abusive emails which may include viruses or inappropriate content.
- Instant Messaging (IM) and Chat Rooms – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity.
- Social Networking Sites – typically includes the posting or publication of nasty or upsetting comments on another user’s profile.
- Online Gaming – abuse or harassment of someone using online multi-player gaming sites.
- Mobile Phones – examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people.
- Abusing Personal Information – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person’s permission.

Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator and pupils should be reminded that cyber-bullying can constitute a criminal offence. While there is no specific legislation for cyber-bullying, the following may cover different elements of cyber-bullying behavior:

- Protection from Harassment (NI) Order 1997 http://www.legislation.gov.uk/nisi/1997/1180
- Malicious Communications (NI) Order 1988 http://www.legislation.gov.uk/nisi/1988/1849
- The Communications Act 2003 http://www.legislation.gov.uk/ukpga/2003/21

It is important that pupils are encouraged to report incidents of cyber-bullying to both the school and, if appropriate, the PSNI to ensure the matter is properly addressed and the behaviour ceases.

Schools should also keep good records of cyber-bullying incidents to monitor the effectiveness of their preventative activities, and to review and ensure consistency in their investigations, support and sanctions.

v. Communication of the School's eSafety policy

Schools should consider and plan for how the policy is to be introduced and shared with all users including teachers, parents, Governors, support staff and pupils. This should include informing all users that all C2k systems are monitored and that security reports can be accessed by school principals.

vi. Email security

C2k recommend that all staff and pupils should be encouraged to use their C2k email system. It is strongly advised that staff should not use home email accounts for school business.

The C2k Education Network filtering solution provides security and protection to C2k email accounts. The filtering solution offers scanning of all school email ensuring that both incoming and outgoing messages are checked for viruses, malware, spam and inappropriate content.

Where staff and pupils use non C2k emails accounts, schools should consider how filtering, traceability and audit ability is achieved.

vii. Internet security

Staff and pupils accessing the Internet via the C2k Education Network will be required to authenticate using their C2k username and password. This authentication will provide Internet filtering via the C2k Education Network solution.

Access to the Internet via the C2k Education Network is fully auditable and reports are available to the school principal.

Where staff and pupils are using non C2k Equipment on a legacy network or if they are accessing the Internet through school provided non C2k connections, schools should ensure that they take appropriate measures to safeguard this equipment against security breaches, as this equipment will not be protected

by the C2k Education Network device security software. Access via this method will also not be subject to the traceability and auditability that is afforded to the C2k managed equipment.

Review and Amend your School's AUP

4.2 Internet access, monitoring and security measures should be utilised by the school where appropriate and these should be highlighted in the school AUP. Staff and pupils need to understand that the use of the school's information technology resources is a privilege which can be removed.

4.3 All users should be expected to adhere to a clear Acceptable Use Policy that is reviewed annually. This policy should remind all users of their responsibilities whenever they are using the Internet and include generally accepted rules of ICT etiquette.

4.4 Sample AUPs are available on the DENI website at: http://www.deni.gov.uk/index/support-and-development-2/internet-and-wifi/management-responsibilities-in-schools.htm and supporting materials/guidance are available via C2k Exchange.

5. C2K and ESAFETY

5.1 C2k provides every pupil and member of staff with a unique username to access C2k services. Authenticated users are granted access to C2k's filtered internet service. User activity is logged and reports of usage are available to nominated staff within a school. Where a school suspects inappropriate use of the internet, the facility to remove access for a user exists.

5.2 Schools need to consider how access is authorised and controlled when offering an alternative broadband provision.

5.3 Schools need to consider how access is controlled in other devices such as mobile phones and other mobile devices using, for example, 3G (Mobile policy).

5.4 The new C2k wireless service enables schools to introduce new technologies to support teaching and learning. These new technologies should be examined for educational benefit and a risk assessment carried out before they are purchased or used in classrooms.

5.5 The school eSafety policy should be updated when new technologies are introduced and after a risk assessment has been completed.

6. SECURUS

6.1 C2k and the Department are looking into the use of a new product that is part of the C2k contract.

6.2 As the new service provides users with more access to online environments, security becomes more important. 'Securus' is an eSafety monitoring system that helps teachers identify cyber-bullying and other child protection concerns. On detection of inappropriate words or phrases, an alert is sent to nominated individuals (pastoral staff) to allow immediate intervention and action.

6.3 It will be provided as part of the new C2k Education Network to assist schools monitor online behaviour. Using such a monitoring system will act as a deterrent and safeguard pupils. This is an additional measure to protect teachers and pupils and support a more open approach to web access. It is currently used by 2000 schools in the UK and the Department is considering a pilot of some schools for this product.

7. AUDIT OF NON C2K NETWORKS

7.1 The Department of Education recently (October 2013) asked C2k to undertake a survey of schools regarding their non C2k provision. Some information on the survey results is provided below:

- Of the 449 responses received 82 schools (18% of those who responded) indicated that they have a non C2k network which accesses the internet and of those not all of them allow pupils access via their non C2k network.
- Respondents reported a wide range of non C2k devices including for example PCs, laptops, iPads, iMacs, Netbook, Kindles etc.

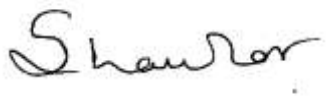
7.2 The Department wishes to draw attention to the findings of the survey which indicate that a number of schools are using non C2k networks/devices. School authorities should ensure that adequate steps have been taken to protect pupils when using non C2k networks/devices.

7.3 Boards of Governors of grant-aided schools have a duty to safeguard and promote the welfare of pupils and to determine the measures to be taken at a school to protect pupils from abuse. In exercise of these duties, Boards of Governors must ensure that their schools have a policy on the safe, healthy, acceptable and effective use of the Internet and other technology tools. They must also actively promote safe and acceptable working practices for all staff and pupils.

8. SOCIAL MEDIA

8.1 As stated above under the heading of Cyber Bullying, recent changes to the criteria used to allow information to be uploaded to social media sites raises particular concerns for children and young people, particularly in relation to access to social media sites outside the C2k service.

8.2 Care should be taken when making use of social media for teaching and learning. Each of the social media technologies can offer much to schools and pupils but each brings its own unique issues and concerns. Each social media technology that is to be utilised should be risk assessed in the context of each school situation.



SHARON LAWLOR
Head of Curriculum Support Team