Department of Education
www.education-ni.gov.uk

Subject:

ONLINE SAFETY

Circular Number:
2016/27

Date of Issue:
01 December 2016

Target Audience:

- Principals and Boards of Governors of all Schools;
- Education Authority;
- Council for Catholic Maintained Schools;
- Northern Ireland Council for Integrated Education; and
- Comhairle na Gaelscolaíochta
- Governing Bodies Association
- General Teaching Council for Northern Ireland
- Teachers' Unions

Governor Awareness:
Essential

Status of Contents:
Advice

Related Documents:

DE Circular 2011/22
DE Circular 2013/25
DE Circular 2015/21
DE Circular 2016/26

Summary of Contents:
This circular provides a set of guiding principles for keeping pupils and the wider school community safe online and for prioritising online safety within the school's preventative education curriculum and overall Safeguarding Policy.

Superseded Documents:
Not applicable

Expiry Date:
Not applicable

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

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

Email: curriculum.supportteam@education-ni.gov.uk

DE Website:
http://www.education-ni.gov.uk

Additional copies:
Tel 028 9127 9543

BACKGROUND

1. This Circular provides a set of guiding principles for keeping pupils and the wider school community safe online and for prioritising online safety within the school's preventative education curriculum and overall Safeguarding Policy.

CONTEXT

2. Online safety, in all cases, in schools and elsewhere, remains a paramount concern. Schools play a crucial role in raising awareness of the risks, highlighting the impact of behaviour when engaging with online technologies and educating children and young people about how to act appropriately and stay safe.

3. We want pupils to have the opportunity to avail of all the positive benefits that come from learning, exploring and connecting with each other online. However, in doing so, they need to know how to protect themselves.

4. It is essential that pupils and adults are kept safe online whilst in school and on school-organised activities. Schools have a responsibility to ensure that there is a reduced risk of pupils accessing harmful and inappropriate digital content. Schools should be energetic in teaching pupils how to act responsibly and keep themselves safe in the digital world and as a result pupils should have a clear understanding of online safety issues and be able to demonstrate what a positive digital footprint might look like for themselves.

5. The school's actions on and governance of online safety must be reflected clearly within the school's safeguarding arrangements and Online Safety Policy. Safeguarding and promoting pupils' welfare around digital technology is the responsibility of everyone who comes into contact with them in the school or on school-organised activities.

Safeguarding Board for Northern Ireland (SBNI) Report (January 2014)

6. In January 2014, the SBNI published its Report '*An exploration of e-safety messages to young people, parents and practitioners in Northern Ireland*'[1] . The report points to a number of important factors which should be taken into account in considering the guidance in this Circular, not least that young peoples' extensive use of technology leaves no doubt over the importance of online safety.

7. Children and young people have a right to be protected and educated. The report highlights the requirement to take appropriate preventative action to protect children and minimise the associated risks around online safety. These risks have been defined under four categories:

[1] SBNI Report 'An exploration of e-safety messages to young people, parents and practitioners in NI

- **Content risks**: The child or young person is exposed to harmful materials.

- **Contact risks:** The child or young person participates in adult-initiated online activity and/or is at risk of grooming.

- **Conduct risks**: The child or young person is a perpetrator or subject to bullying behaviour in peer-to-peer exchange and/or is at risk of bullying, entrapment and/or blackmail.

- **Commercial risks**: The child or young person is exposed to inappropriate commercial advertising, marketing schemes or hidden costs/fraud.

INDICATORS OF POOR ONLINE SAFETY PRACTICE

8. Some indicators of poor online safety practice include:

    - Pupils are not aware how to report a problem.

    - Password security is ineffective and passwords are shared amongst teachers and pupils and between pupils.

    - Policies are generic and do not accurately reflect what is going on in each school in terms of the use of technology.

    - Online safety is treated as a separate policy rather than being integrated into existing safeguarding/child protection, behaviour, code of practice, anti-bullying policies.

    - There is no planned or progressive online safety curriculum or education provided in the school.

    - There is no Internet filtering or monitoring of Internet use.

    - There is no evidence of regular staff training on online safety.

    - Personal data is often insecure leaving the school with insufficient knowledge about who can access the data or how it is being/can be used.

CHARACTERISTICS OF GOOD ONLINE SAFETY PRACTICE

9. This section sets out, under various headings, some of the characteristics of **good online safety practice**. These are intended to help schools in developing or reviewing their own practices and procedures.

Policy

- Online safety forms an integral part of the school's safeguarding/child protection policy and is approved and monitored by the Board of Governors.

- Policy and procedures about online safety are integrated into existing safeguarding/child protection, behaviour, code of practice, anti-bullying policies.

- There are clearly defined procedures for reporting and dealing with incidents surrounding breaches in the school's online safety guidelines.

- The online safety section incorporates agreements on the acceptable use of:

    - the Internet and school-based Digital Technology.
    - Personal Mobile Technology.

- There are clearly defined procedures for reporting and dealing with incidents surrounding breaches in the school's Online Safety guidelines.

A Consistent Whole School Approach

- All teaching and non-teaching staff can recognise and are aware of online safety risks.

- Online safety messages are integrated across the curriculum for pupils in all Key Stages.

- Online safety messages are distributed amongst pupils, staff, parents/carers and the wider community.

- The school's leadership and management have clearly prioritised online safety and safeguarding across all areas of the school.

- Knowledge is shared amongst staff and there are good capacity-building opportunities.

Staff Education

- School staff receive appropriate online safety training and regular online safety information.

- One or more designated members of staff have a higher level of expertise around online safety.

- Safeguarding and child protection training, including online safety, is given to all staff.

Education of Pupils

- Pupils receive age-appropriate online safety messages that are relevant and engaging.

- The school actively promotes online safety messages for pupils on how to stay safe; how to protect themselves online; and how to take responsibility for their own and others' safety.

- Online safety is actively promoted within the school, for example through the development of online safety messages by the learners themselves, and participation in events such as Safer Internet Day and associated competitions organised by agencies such as EA/C2k.

Education of Parents and Wider Community

- The school makes parents and carers aware of important online safety messages via appropriate training providers.[2]

- Regular and relevant online safety resources and messages are offered and shared with parents via the school website and social media where appropriate.

Monitoring & Evaluation

- As part of its Safeguarding policy, it would be good practice for the school to keep an up-to-date record of potential breaches of online safety in an Online Safety Risk Register.

    - It is recommended that the Principal approves staff access to modules in SIMS. It should be understood that access to System Manager in SIMS opens up access to the entire SIMS database.

Management of Personal Data

- The school has effective policies and procedures in place which ensure personal data is collected and managed responsibly in line with relevant

[2] Advice and links to appropriate training providers is available via the C2K Online Safety Fronter page. Some schools have provided excellent training to parents through student-led workshops and presentations.

legislation, namely the Data Protection Act 1998 and Freedom of Information Act 2000.

- All communications between the school and pupils, their families/carers and external agencies delivered using technology should be clear and professional.

- The school has a clear process for transferring data to third parties. Advice on this is contained within DE Circular 2015/21[3].

Reporting

- There are robust report channels in place for reporting online safety issues and pupils and staff know who they can turn to if there is a problem. Instances relating to child protection should be communicated to the designated teacher. More advice is available in the Safer Internet area within Fronter, a component part of the C2k EnNI service.
- In cases of Internet abuse or where a child is at risk the school's child protection procedures should be implemented.

SOCIAL MEDIA

10. Social media provides an excellent vehicle for communicating directly with parents/carers and the wider community.

11. An increasing number of schools now have their own social media accounts. However, most social media platforms have a recommended 13-years lower age limit which would rule out the direct use of social media for primary school pupils.

12. While many younger pupils will not be able to engage in social media directly, making them aware that the school and their parents/carers are interacting via social media gives them the opportunity to see that social media can be extremely positive when used in a responsible manner.

IMPORTANT ADVICE REGARDING ONLINE FILTERING RESPONSIBILITY

13. EA/C2k has procured and provides a filtered Internet service (see Filtering) for and on behalf of all pupils and staff in schools in Northern Ireland. This is provided as part of the core C2k EnNI service in all schools. It is the Department's view that the provision of this filtered Internet service should remove the need for any school to continue to have a second line/network in place.[4] DE's direction of 2014 is reiterated explicitly through this Circular.

[3] DE Circular 2015/21 - School obligations to manage data

[4] DE letter to schools 18 September 2014

14. Where a school decides to provide alternative Internet access, then the responsibility for the effective filtering of any inappropriate online content rests with the school's Board of Governors. This is unless otherwise agreed in a written contract with the service provider.

15. The school's senior leadership team must take effective measures to ensure that any alternative Internet provision does not undermine or adversely impact on the overall effectiveness of the school's child protection and safeguarding policies.

MOBILE TECHNOLOGIES

16. The Department has issued a separate Circular (DE Circular 2016/26) that provides advice and guidance on effective uses of mobile digital devices for teaching and learning.

RECOMMENDATIONS FOR SCHOOLS

17. As well as considering the characteristics of good online safety practice detailed under Point 9 above, listed below are some recommended good practice actions for schools in developing or reviewing their online safety provision.

    - Schools should demonstrate a clear understanding of their current online safety provision by auditing their current provision. Evidence of this audit should form the basis of the online safety section contained within the Safeguarding policy. An example of this audit is available by registering on the *360 degree safe* website.[5]

    - Schools should review and develop safeguarding procedures and the roles of staff responsible for advising and reporting on online safety concerns.

    - Schools should audit staff training needs on a regular basis and identify suitable updates/courses for the information of/attendance by key members of staff.

    - Schools should communicate important online safety advice, concerns and current issues to parents and carers.

    - Schools should deliver an age-related online safety curriculum to enable pupils to become safe and responsible users of technology.

    - Schools should operate a 'risk register to record possible online safety issues and highlight where data security might be potentially breached.

[5] the link is available in the Online Safety area in Fronter

- Schools should also operate a 'Register of Access' which clearly outlines who has access to the different pupil and staff data available of the school system. A sample copy of a 'Register of Access' is available in the Online Safety room in Fronter.

- Schools should, as an integral part of their behaviour policy and staff code of practice have acceptable use agreements in place for pupils and staff on using the internet, school-based technologies and personal mobile devices which may, in the case of pupils be signed by parents/carers.

THE SERVICE PROVIDED BY C2K

18. To underpin the advice in this Circular, C2k provide the following services to all grant-aided schools in order to facilitate the process of safeguarding children.

Filtering

19. Filtering on the C2k network is grouped as follows:

    - Internet Advanced – allowing access to a wider range of pages than the default including webmail, shopping, drugs and alcohol, sex education.

    - Internet Streaming – allowing access to streaming media websites including Youtube, BBC iPlayer, Vimeo, TV and radio streaming sites.

    - Internet Social Networking – allowing access to social networking sites including Facebook, Twitter, LinkedIn, Wordpress.

20. In addition, C2k, through the managed service provider, adhere to ISO 27001 standard security around the C2k EnNI system:

    - Forcepoint (formally Websense) filtering in place for Internet access.

    - Nightly Internet Watch Foundation (IWF) updates.

    - Option to sign up to Delegated Access. This provides the school with more control over their own Internet filtering. Inappropriate websites remain blocked. Delegated access offers schools the facility to report on Internet usage without going through the Service Desk.

    - All staff and student/pupil internal and external email is filtered for inappropriate content.

Monitoring

- The Principal or appointed Senior Staff can request an Internet Usage

Report for any pupil or member of staff using the core C2k EnNI service. Schools are asked to ensure that the individual has signed off on the acceptable use agreement in which it is expressly mentioned that these reports may be requested.

- Securus is currently in pilot mode in schools but when rolled out will monitor the screen display and keystrokes alerting schools that a student may be at risk or in breach of acceptable use. Some of the issues and concerns that Securus detects include:

  - Cyberbullying
  - Online grooming and child abuse/exploitation
  - Depression, self-harm and suicide
  - Racial, homophobic and religious harassment
  - Use of drugs or weapons
  - Attempts to use a proxy bypass to access restricted sites

ARBITRATION

21. The C2k Service Desk is open for requests from schools who wish to have websites and specific keywords opened up through the current C2k filtering policy. Successful arbitration of these addresses will be based on careful consideration of the Terms & Conditions of the specific websites. Consideration will be based on protecting the school from breaching safeguarding principles. Schools may be asked to submit further evidence through the school Principal stating the educational benefit in opening up the website or keyword.

FURTHER SUPPORT & ADVICE

22. Further documentation, links to the 360 degree safe website, online safety template and sample acceptable use agreements can be found in the Online Safety area in Fronter.

23. The Department's webpage on online safety provides further advice and links to relevant DE Circulars sites providing advice for pupils, parents and teachers.

    education-ni.gov.uk/keeping-children-safe-online

24. The Education Authority Safeguarding site provides useful information on all aspects of safeguarding and child protection:

http://www.eani.org.uk/schools/safeguarding-and-child-protection/