

Freedom of Information – Response - 2025

This request relates to the safe use of the Internet by primary and secondary school pupils in your region. Resources:

1. *The Byron Review, published 27 March 2008.*
2. *The Byron Review Action Plan, published 24 June 2008.*

The resources above relate to the safety and education of children using the Internet at home and school, and the responsibility of government, local and national, to ensure that children are educated and protected whilst doing so.

I hereby request under the Freedom of Information Act full details of the Internet Safety Actions and Initiatives currently in place throughout the region.

1. Internet Safety Education provided as part of the school curriculum.

Within your schools is there a specific program aimed at teaching children about staying safe online, including cyber bullying, been integrated into the curriculum?

Response:

The reference to a 'program' here suggests a computer program rather than a 'programme' which would mean a module of work or a project focus. In relation to this, we would not be condoning any particular approach with a particular piece of software. However, we do support a process approach to schools in relation to internet safety in the following ways:

- Using Becta (formerly known as the British Educational Communications and Technology Agency) materials to help schools develop a process approach to e-safety and acceptable use that includes everyone (see next section).
- The Personal Social Development team is running a pilot with several schools called 'Learning Together, Working With Parents' which is focusing specifically on e-safety; and they are also running a conference in November concerned with anti-bullying of which cyber-bullying will be an integral part. This will aim to develop a student network with Y8 and above students specifically looking at anti-bullying.

If yes, who is responsible for delivery and what accreditations/training have they received? For example, teacher, Child Exploitation and Online Protection trained ambassador.

Response:

Clearly, schools are responsible for setting up and delivering an acceptable use policy, (reference: Safeguarding children online - a guide for school leaders, Becta). To this end Inclusive School Improvement Service run workshops to support this work which is advertised on our CPD (Continuing Professional Development) Web site:

www.suffolkcpd.co.uk.

There are also several 'boards' and training opportunities that guide approaches to e-safety, (the LA e-safety board, the E2bn* Regional broadband e-safety group and [e2bn](#) e-safety conferences). There is also a multi-agency e-safety steering group which is made up of members from organisations like Becta, NSPCC, Suffolk Colleges, Connexions, schools, Inclusive School Improvement Service, safeguarding board and library services. Some Police Education Partnership officers are trained as Child Exploitation and Online Protection ambassadors.

*E2BN is the Learning Grid for the East of England and regional provider of the National Education Network. E2BN supplies schools with broadband services and innovative online learning projects.

If yes, how often is internet safety training integrated into the school curriculum, i.e. weekly, monthly etc.?

Response:

Schools are now expected to integrate e-safety work into their curriculum. For example, key stages 3 and 4 ICT National Curriculum makes specific reference to e-safety (in both key stages: *Section 2: Key processes* – 'Developing ideas' and 'Communicating information' contain mandatory references to e-safety).

The new [OFSTED](#) guidance refers to 'The extent to which pupils feel safe' and categorises schools in their approaches to the extent to which e-safety processes are integrated into the school under the five main headings (Overall Effectiveness, Achievements and Standards, Provision of Curriculum and Teaching and Learning, Leadership and Management, and Training). The current SEF requires schools to respond to safeguarding issues.

If no, what steps/timeframes are being taken for implementation?

Response:

Not applicable.

2. Internet Filtering

Do the primary and secondary schools within your authority have internet filtering in place?

Response:

All schools using the local authority broadband service have internet filtering in place.

If yes, what tools do you use? For example Hardware or Software?

Response:

Filtering is provided centrally by an array of managed Web filtering and caching appliances. Direct access to the Internet is blocked on our exterior firewall.

If yes, what is the name of your internet filtering supplier and when was their contract last renewed/due for renewal?

Response:

The contract was last renewed in 2009. Due for renewal in 2015. Supplier is East of England Broadband Network.

3. Internet Filtering Breaches

Have any of the schools within the past 24 months experienced a breach of Internet Filtering where children were able to access pornography or Indecent images. Please provide details of School Type (primary or secondary), Date of Breach and Type of Unsuitable material accessed.

Response:

None reported to Suffolk County Council. Blocking requests are made directly by schools to our supplier. We do not regard blocking requests as a breach of Internet Filtering.

Our supplier reports that:

"There were just 20 block requests that may be relevant in the 24 month period, 18 from secondary schools and 2 from primary. We are unable to provide a list of dates as the records contain personal data, however, the reports are spread over the whole 24 month period. It should be noted that this number of requests relates to the number of block requests from Suffolk schools' personnel including teachers and support staff, they do not necessarily mean that children have accessed an unsuitable site as the issue may have been picked up by teachers or school support staff who have a greater degree of Internet access than students.

We do not regard these as a breach of filtering, they are part of the normal process of feedback and refinement.

We are not sure how the requester distinguishes between Porn and indecent images, all the 20 requests above were classified as porn. However, we have had no (zero) reports from any school of illegal images being accessed by children."

If a breach of security occurred how your authority was notified? For example, by a parent, by the school, through an automated alert provided by hardware/software supplier.

Response:

Not applicable as none reported.