CIT Statement for the meeting of DfE Filtering and Monitoring Standards:

Technical information:

The Trust has implemented SENSO as the chosen monitoring software.

Filtering system is called 'Securly'

SENSO is on the DFE directory of UK monitoring providers. SENSO is configured to send an email including a screen shot and user details to the DSL if a student access inappropriate content. The DSL will the investigate and resolve appropriately. The IT staff will be notified to action an immediate internet ban and blocking of websites Safety Tech Providers.

IT Lead is responsible for maintaining the effectiveness of filtering and monitoring systems across the Trust. The Lead IT is responsible for the procurement of the filtering and monitoring across the trust and meets regularly with the IT support company and the filtering company to ensure inappropriate sites are blocked.

Strategic Information:

In individual schools, the effectiveness of all internet filtering and monitoring comes under the overarching umbrella of safeguarding. This assurance is the responsibility of the DSL to check and to report any concerns to the relevant school and Trust leaders.

Our board have delegated a series of assurances to local school boards – LSBs, to provide information to the board via regular systemic reporting systems. Safeguarding is one of the LSB delegated assurances.
The Trust board have overall strategic responsibility for filtering and monitoring and require from schools an assurance that the standards and responsibilities against the required standards are being met.
The operational effectiveness of internet filtering and monitoring PLUS the consistency of response from staff and pupils to breaches in individual schools is part of the assurance from the LSB to the Trust Board.
The Trust has provided a document for all schools (see attached) that shows how we meet the required standards.
Our systems and procedures are reviewed annually by our central IT team. This is informed by information contained in LSB and headteacher assurances. LSBs will share this information through their regular existing reporting arrangements under the umbrella of their Safeguarding information.

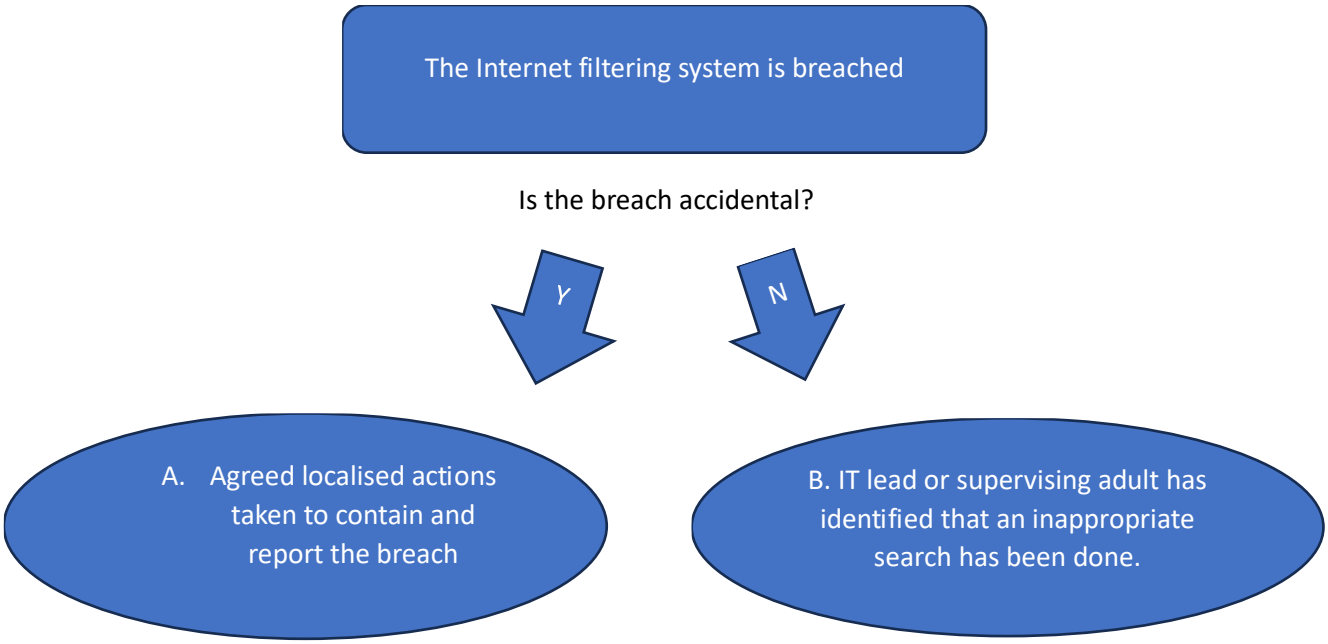
How breaches will be found:

SENSO will send a notification to named safeguarding leads in schools to identify when a search has been done that meets the criteria for a blocked search. i.e., contains whole or part words that are designated problematic. The Trust expects that DSLs will aim to check these emails daily at least once before the close of school, however we appreciate that in a busy setting this might not always be manageable. There is an expectation that they will be checked at least every other working day.

Leaders must check before the end of school ahead of the weekend and before a holiday. This is to ensure that if a significant term has been searched for that could indicate a significant risk of harm, is detected before a weekend or holiday – for example any sites relating to issues such as drug-taking, self-harm, suicide, extremism etc that could indicate an intent to harm self or others. This list is not exhaustive, and will be governed by the context and community that the school serves.

Once notified - schools will have a consistent, rapid localised response to the strategy they adopt when firewalls and filters are breached by inappropriate content. This includes if the report of a breach comes from a member of the school community rather than from SENSO – if a child tells an adult they have seen or typed something that is inappropriate.

In all cases the DSL will triage the concern and assess whether the search was accidental (for example as a typo, or the alert was triggered by a 'part word' that was part of a bigger word that in its entirety does not pose a concern). See below:



Subsequent actions to be taken by leaders:	**A – accidental breaches** **If the report has been received from a pupil:** Written report received from supervising teacher containing the information what, when and by whom. DSL to talk to pupil to check whether the search content was accidental/typo/etc. DSL to ensure the pupil has followed the school agreed system to ensure the breach is contained. The breach to be recorded on the school MIS under a tab categorised as SENSO. DSL to contact IT to let them know what has got through if it has not been picked up by SENSO. IT team will take action to remove and block. **If the breach was identified by SENSO:** DSL to talk to pupil to check whether the search content was accidental/typo/etc. DSL to ensure the pupil has followed the school agreed system to ensure the breach is contained. The breach to be recorded on the school MIS under a tab categorised as SENSO.	**B – Non-accidental breaches** **There may be a significant safeguarding concern if a child is searching for inappropriate terminology. Leaders must proceed with this in mind.** **If the breach is identified by a pupil or adult in school:** Adult to make a MIS (CPoms/Schoolpod) report to DSL to show what who, what, when. DSL to triage the concern. DSL to take appropriate investaigatory activities accordign to the safeguarding policy. **If the breach was identified by SENSO:** SENSO email alerts will be checked daily, according to schoola greed routines. If the breach has been identified by SENSO, the school leaders must be informed and the DSL will investigate and take the appropriate action as agreed by the SLT to safeguard the individuals.

What is the expected response from staff and pupils if the filters are breached:

Schools MUST have an agreed procedure that kicks in consistently across the school if a child sees or opens something inappropriate on any device in school.

All staff and pupils must be aware of this process and can explain it clearly as well as use it.

This strategy should include:

- How other children are protected from seeing inappropriate images i.e., they know to immediately close the laptop or turn the screen off.
- How they make sure an adult knows they have seen something that makes them feel uncomfortable (learning about what is appropriate and what is not, should be part of the E-Safety curriculum)
- What adults then do with that information.

Any accidental breaches of the filtering system MUST be noted and passed on to the DSL who will ensure the IT team at the centre are aware (see diagram above).

The central IT team will block any sites or content that are reported by schools.

Our School Strategy is as follows:

At Boston Endeavour Academy we use the acronym **HELP.** This stands for:

H Hide the screen

E Explain what you have seen to an adult

L Leave the laptop or computer and don't go back to it

P Plan the next steps

Posters are displayed in the Computer Suite and in the relevant classes. The acronym has been explained to students where appropriate. The posters are referred to regularly when students are accessing technology. Online safety is covered within the RSE curriculum, assemblies and workshops delivered by the Stay Safe Partnership.