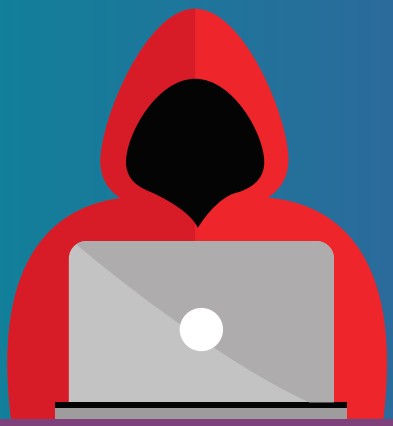
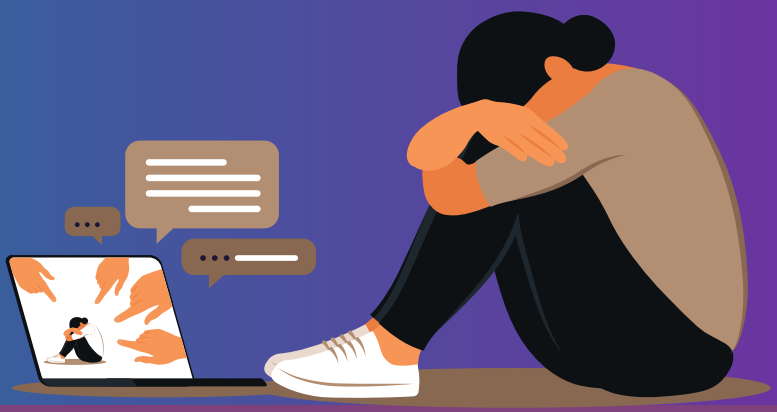
Securus
Safeguard Monitor Protect

Four online safety scenarios in schools *that happen more than you think* and how to avoid them





Free safeguarding support pack for school DSLs

Securus
Safeguard Monitor Protect

FOUR ONLINE SAFETY SCENARIOS IN SCHOOLS THAT HAPPEN MORE THAN YOU THINK **AND HOW TO AVOID THEM**

Welcome to your free digital safeguarding pack - a compilation of real-world digital safeguarding scenarios that we know take place in schools every single day. Last year, in a 12-week period across 50+ schools, we helped capture 140,000 potential online safeguarding incidents including those related to grooming, hacking, eating disorders, terrorism, mental health and pornography.

On their own, the digital safeguarding scenarios in this pack make extremely valuable staff training talking points to assess staff knowledge and identify any potential training gaps.

Alongside the scenarios, we show how Securus' monitoring and reporting software would significantly mitigate the types of risks exposed. We also offer actionable steps that DSLs can take immediately - irrespective of purchasing Securus - to help keep pupils a bit safer.

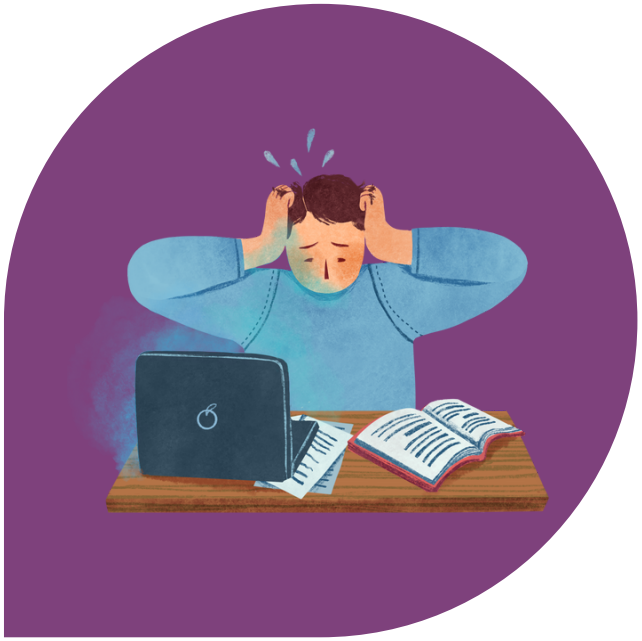
We hope you find the resource useful.

The Team at Securus Software

Email: enquiries@securus-software.com
Tel: (0)330 124 1750
Visit: www.securus-software.com

Follow us on social

SCENARIO 1:
Online Radicalisation



"Children under the age of 18 made up 13% of all terrorism arrests in the year to 31st March 2021"

The scenario

A student comes from a stable family background, is high performing across all subjects and well behaved in school. No safeguarding issues have ever been detected by any member of school staff. However, in recent months, the student is being groomed by an unknown religious group who are trying to indoctrinate its extremist views with the view of recruiting the student into hate crime.

The student has been researching themes linked to extremism and radicalisation on devices in the school library. However, because they have been using approved websites such as the BBC, their online activity continues to go unnoticed because the school only has a web filtering product in place. This does prevent the student from accessing some websites, although the school is unable to identify who might be still trying to access these sites and how often. The student repeatedly visits online articles on school-approved websites discussing extremist ideologies.

Act Early Campaign - www.counterterrorism.police.uk/

Reducing the risk

The BBC is considered the most trusted international news brand with 1.5 million page views reported in March 2020. Many schools' web filtering systems include online newspapers and media distributors on their list of 'safe' or 'approved' websites.

The trouble is web filtering can't distinguish between context and nuance. If your students are repeatedly accessing online articles from BBC about extremism, self harm or substance abuse - **would you know?**

Securus works with schools' existing web filtering systems to enable unlimited web access to students but with the highest level of safety measures in place. We **capture screenshots of students' devices** as soon as it detects a word/phrase from its extensive library whenever it is keyed in via the keyboard or even just viewed on screen. It then automatically sends a report to the DSL. Our software also reduces the amount of false positives, which means schools don't have to put a blanket ban on certain websites if those websites can provide educational value.

Take immediate action

Below are 3 things DSLs can do right now to help **mitigate risks of online radicalisation.**

1. Filtering versus monitoring? Keeping Children Safe in Education stipulates schools must "ensure appropriate filters and appropriate monitoring systems are in place and children should be prevented from accessing harmful or inappropriate material." Every school will have web filtering in place, but ask whoever is in charge of your school IT, how you **monitor** students' online activity? Filtering and monitoring are not the same - but you must ensure you have both.

2. Self review online safety: Complete a self-review of your online safety measures to help identify any potential safeguarding gaps in your web filtering, monitoring or reporting. There are lots of free tools available for schools including 360safe.org.uk

3. Learn to spot the early signs: Do you feel confident spotting the early signs of anti-hate or terrorism behaviour? The Action Counters Terrorism (ACT) website offers some great information to help prevent pupils harming themselves or others.

SCENARIO 2:
Bullying via Offline Applications

"Young people (10-16 years) who accessed or shared sexual content or images of cyberbullying or violence had up to a 50% higher risk for thoughts of suicide"

The scenario

A student is receiving abusive and threatening messages from another student during school hours. To avoid detection and to get around the school's ban of social media and messaging apps, the perpetrator - another student - is creating messages in MS Word, as well as derogatory images in MS Paint, then attaching these documents to emails and sending them to the victim. The victim is extremely frightened by the messages and worried about the repercussions if they seek help so chooses to remain silent. As a result the messages increase in frequency and levels of intimidation.

Reducing the risk

Online bullying remains extremely high on every DSL's radar but it's likely that most teachers will have only considered online applications (e.g. social media) as the means to conduct this kind of child-on-child abuse.

'Association of Online Risk Factors With Subsequent Youth Suicide-Related Behaviors' - jamanetwork.com/

Online applications - such as commonly used Microsoft tools - can also pose a safeguarding risk. And of course they will not be blocked or detected by most school web filtering systems. Securus monitoring software detects safeguarding risks across online and online applications such as MS Word, PowerPoint, Google Docs and Mac Pages through sophisticated screen capture technology. Securus' character recognition design means it can detect words and phrases irrespective of application or setting including online activities.

Even where students can't or won't report peer-on-peer abuse using online applications, Securus Software will monitor and capture incidents 24/7 and send these to the DSL.

Take immediate action

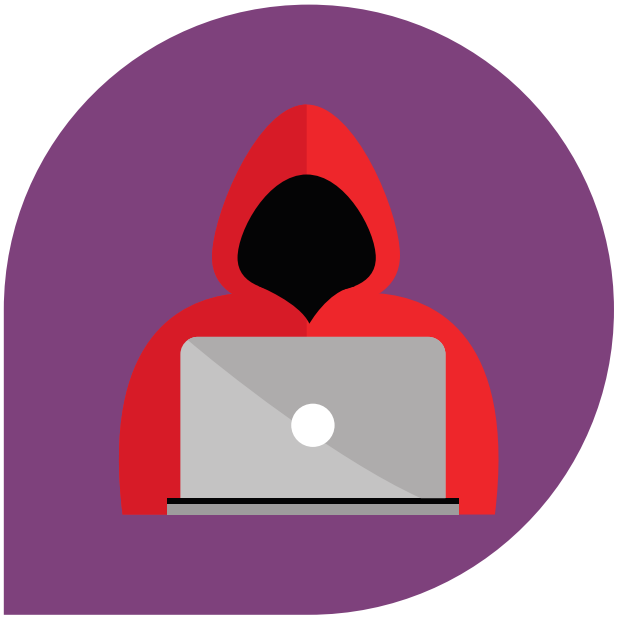
Below are 3 things DSLs can do right now to help **mitigate risks of child-on-child abuse via online and offline applications.**

1. Reporting an incident: Check that all students know where to go/who to tell if they are concerned about any type of online or online bullying? Are they aware of CEOP's Child Protection Advisors? Also, would they actually seek support if it happened to them (asking this in itself can be extremely valuable from a safeguarding staff training point of view)?

2. Be aware before you share: Child-on-child abuse such as revenge porn can take place through social media and messaging apps but also be carried out using online applications if images are edited and printed out. There are some useful free resources on the Gov.uk website as part of its 'be aware b4 you share' initiative.

3. Apply online safety measures to your online applications: Pupils have been known to use MS Word to outline plans for self harm or the intention of suicide, hence the importance of online monitoring performance. This might simply be a coping mechanism or signs of something far more serious. Any bullying incidents that take place, whether online or online should be dealt with to protect both the victim and the bully. In many instances, the bully may also be suffering from issues either at home or amongst peer groups and DSLs may need to offer support to both parties for very different reasons.

SCENARIO 3:
Student Cyber Criminality



"Research by the UK's National Crime Agency (NCA) suggests that people as young as 12 years old could be at risk of becoming involved in cyber-dependent criminality"

The scenario

A particularly tech-savvy student who received a DfE-funded laptop from his school during the pandemic, regularly commits seemingly low level incidents of cyber crime in his spare time. This includes things like using 'booter' tools to knock other online gamers offline so he can win a particular game, as well as using friends' online login details to play pranks on them.

With 'anytime' access to his school network, on a couple of occasions, he has attempted to circumvent the school's IT security via proxies or 'task kill' for the thrill of the challenge and 'just for a laugh'. This has resulted in interfering with the school's IT security, which leaves it susceptible to other hackers. However, more frequently, he attempts to increase his user privileges and access restricted data on the school network such as staff HR files and test answer forms, and he shares some of his 'wins' with friends.

The student has disrupted lessons on several occasions because of computer misuse and taken up valuable IT resources to sort things out.

'Young people and cyber criminality' - www.getsafeonline.org/

Reducing the risk

Students' computing skills are becoming increasingly more sophisticated and since more devices have been issued for use at home, students now have a big advantage when it comes to circumventing the school network. Securus software can detect these actions and alert the school providing details of the student's name involved, which gives DSLs and other SLTs greater ability to intervene.

Similarly, Securus can identify when multiple attempts are made to use a compromised password. Checking the finer details of each case, the student that carried out the initial 'hack' can be identified and spoken to with implications of such hacks explained.

Take immediate action

Below are 3 things DSLs can do right now to help **mitigate risks of student cyber criminality**.

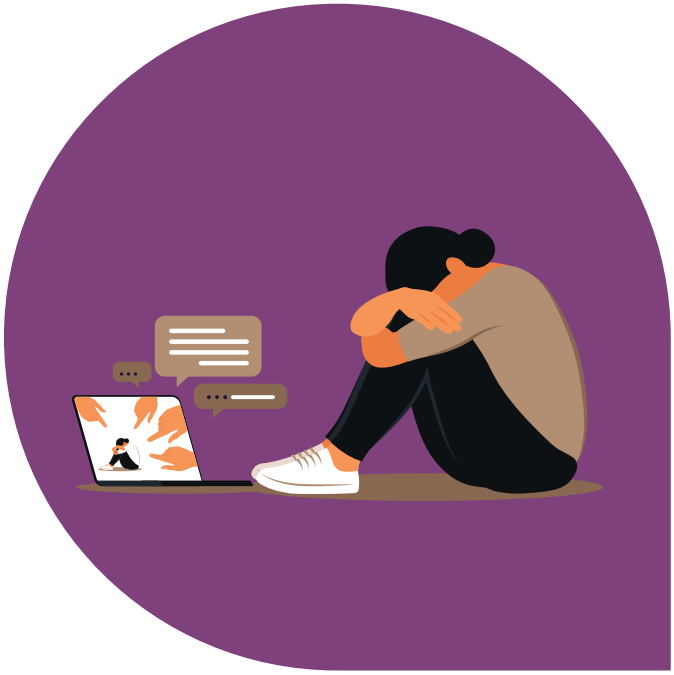
1. Petty cyber-crime: Educate students on the risks and consequences of seemingly low-level cyber crime. The National Crime Agency has some useful free resources. If you are concerned that a student is making the wrong cyber choices, you should contact the Cyber Prevent team in your local Regional Organised Crime Unit (ROCU).

2. Cyber security risk register: Check that your core IT services are included in your cyber security risk register - ask your School IT or Network Manager, or IT Managed Services Provider, to assist you if necessary. It is also worth a conversation with your SLT and School Business Managers about a business continuity plan should you suffer a DDOS attack - less than half of schools currently include this.

3. Password integrity: To help protect password integrity, ask your School IT or Network Manager to enter previously compromised root /system passwords into your web filtering library so they can track individuals who are attempting to disrupt or attack the core network.

SCENARIO 4:
Self Harm and Non-Typed Incidents

"A national inquiry into suicides by young people found there was suicide-related internet use in nearly half of suicides by young people every year"



The scenario

A student from a school with a BYOD policy brings her personal iPad to school regularly to help with her learning. The student suffers from an eating disorder, body dysmorphia and self harm, and becomes increasingly isolated from friends and peers. Instead she spends an increasing amount of time online - including during free periods and in the school Learning Resource Centre.

The school's web filtering system prevents her accessing the majority of potentially harmful websites from any typed search. However, unbeknown to any teaching staff, the student is a regular user of the growing social storytelling platform Wattpad, and is able to access and read triggering stories from both non-typed and online activity on Wattpad.

In addition, the student repeatedly browses and taps on triggering images and related content without actually the need to type anything into her search browser.

Young People, the online environment and suicide - www.samaritans.org/

Reducing the risks

In our experience, most words/phrases that generate screen captures are not typed by the monitored individual. For this reason the importance of coverage and performance in this area is paramount. This is often reflected in Securus' full monitoring service where the majority of high risk incidents reported are in fact non-typed.

The Securus safeguarding team (FMS) have reported that 90% of captures they moderate are non-typed captures. The software continuously scans the screen and even multiple screens for any inappropriate material.

Take immediate action

Below are 3 things DSLs can do right now to help **mitigate risks of non-typed digital safeguarding incidents.**

1. Monitoring for non-typed incidents: Find out from your School IT or Network Manager, or IT Managed Service Provider how students' non-typed digital activity is currently monitored across your school devices? What systems do you have in place given that non-typed digital safeguarding incidents are more prevalent than most teachers think?

2. Monitoring historic data: Ask your School IT or Network Manager if your current safeguarding IT products provide you with the ability to capture pre-existing content?

3. What is WattPad? WattPad is just one of the social networking sites growing in popularity amongst students of all ages so it's worth brushing up on what exactly it is if you're not familiar with it. Protect Young Eyes has a useful article about the safeguarding risks of Wattpad.

WHO WE ARE

Since 2002, Securus has been at the forefront of online safety and monitoring software solutions for the education sector. As a pioneer of digital safety, we have developed leading edge technology to help School Designated Safeguarding Leads improve the way their school protects students from the latest digital safeguarding risks.

WE PUT PEOPLE FIRST

The Securus Team is made up of an incredible number of online monitoring experts who dedicate themselves to keeping children and young people safe from online harm.

Our primary focus is always to monitor, safeguard and protect the welfare and safety of children and young adults.

"We were prompted by our investigation into the recent government requirement to investigate the steps that we take to keep children safe from harm online from cyberbullying, pornography and the risk of radicalisation. We felt that Securus offered us the best possible solution in addressing the requirements of 'Keeping Children Safe in Education' and the needs of our school."

— The Boulevard Academy, Kingston Upon Hull

HOW WE HELP DSLS

We offer a Full Monitoring Service for School Designated Safeguarding Leads who want ultimate peace of mind and protection for their pupils with significantly reduced workload.
Visit: www.securus-software.com/full-online-monitoring-for-dsls/

Our partners

Contact us

Email: enquiries@securus-software.com
Tel: (0)330 124 1750
Visit: www.securus-software.com

Follow us on social