Case study

DSL Information Sheet

Questions for the DSL to facilitate a discussion:

Initial (after reading the case study)

- What went wrong?
- When should action have been taken?
- What would you have done differently if you had been a member of staff at that school?

Secondary (after feedback discussion)

If it happened here:

- Who would you report your concerns to?
- What would you do if they were not listened to/no action taken?

This case study is based on actual events. It's essential that staff know how filtering and monitoring systems work, who is responsible for different elements, and the action to take if they have a concern about a child.

Additional notes to facilitate feedback discussion:

- *TJ is autistic and on an Education, Health and Care Plan.* Children with SEND have additional vulnerabilities which need to be taken into account.
- *At home, devices have strong passwords and her parents sit with her when she accesses the internet.* It is also important to balance the need for protection with the need for children to learn to become safer online, have safe space to make mistakes, and to have an appropriate degree of privacy to explore legitimate age-appropriate topics.
- *The school she attends is judged good by Ofsted, noting that students had plenty of opportunities to learn how to keep safe and healthy through their regular personal, social and health education lessons, including about online safety.* When looking at patterns of absence, it is important to check which lessons are regularly missed, and to seek ways to ensure safety messages are made available to those who have

missed them. Often the children who most need the messages are those who are vulnerable in other ways, such as being absent for repeated or prolonged periods.

- *The school has a filtering system in place for their computers, which has not yet been extended to the iPads. It is not monitored by the DSL.* It is important that every type of device provided by your setting is covered by your setting's filtering system (including those used off-site), and that said system is suitable for the age, understanding and needs of the children in your care. You should also ensure that devices and usage are effectively monitored physically and/or via technical means. The named responsible governor, senior leader and DSL should understand, have oversight of and regularly review your system alongside relevant IT staff and your IT provider in line with DFE guidance. It is also important to consider how 'bring your own devices' are used and managed.
- *In school, TJ often refuses to attend lessons. Sometimes, she only attends one or two lessons a week.* It is important to have a safeguarding approach to behaviour management, ensuring that behaviour is seen as communication, and that efforts are made to identify what lies behind the behaviour. It should not be automatically assumed that behaviours are related to a child's SEND, nor should challenging behaviour be responded to solely by sanctions.
- *When she doesn't attend lessons in class, TJ mostly accesses information from a school computer and a school iPad. She is rarely supervised*. It is important that all children's online access is fully supervised and/or device monitored in line with DfE guidance. Settings cannot rely on filtering alone.
- *At some point, the school's filtering system stops working*. It is important to monitor and regularly check that your system has not changed or been deactivated. A sample of every type of device should be checked, as well as checks being made in different areas of your setting. Devices used by a range of different users (e.g. staff, students, guests) should also be checked regularly. South West Grid for Learning's testing tool can be used for some checks.
- *TJ died by suicide on the same day she accessed a story on an online platform she freely accessed (and which several schools currently allow) which featured an act which she copied.* It is important that filtering systems are robust, use approved block lists etc. and are backed up by effective monitoring. Likewise staff should regularly check the platforms they use and suggest to children for material they may not expect. Settings should exercise control over how children's data is being processed by Ed Tech. EdTech providers should be queried about what protections are applied to their 'Additional Services' and the risks assessed before they are enabled by

settings. All settings should take into account different children's levels of need and vulnerability.