School Risk Assessment: use of AV1 telepresence robot in school classrooms

Supporting children with medical needs to access their education is a vital and challenging part of a school's responsibility. We understand your duty to safeguard children in school, as well as those at home, and also to ensure your teachers' privacy. To help you with this we have created a template risk assessment that you can use to make sure that the use of AV1 within your school is as safe as possible. In preparing this document we have consulted the following government documents, which you may also find useful to refer to;

- Education Act (2011)
- Keeping Children Safe in Education
- Supporting pupils with medical conditions at school
- Realising the potential of technology in education

Overview of the privacy features of AV1

- AV1 transmits a live-stream. No data is recorded. Meaning no legal requirement to collect consent from parents of other students.
- The AV1 live-stream is encrypted end-to-end.
- The AV1 app is password protected, so that only the intended user can log in.
- Only one device can be synced to an AV1 at any one time. A single-use keyword is required to sync a device to AV1. Keywords are sent securely to the customer.
- No Isolation do not require or hold any information on our users, such as age, name, or illness.

Risk Assessment

When using this risk assessment template below, consider **Proximity**, **Impact**, and **Urgency** of each risk.

You may wish to rate each risk out of 3:

Low risk = 1 Moderate risk = 2 HIgh risk = 3

- **Proximity:** How likely is it to happen?
- **Impact**: How bad could it be?
- **Urgency:** How quickly does something need to be done about it?

We hope this helps you as a school leader see any potential risks in the wider context of your school environment, community, and children that you support.

1 Activity	Risk	Considerations	Control measures/ possible actions to reduce risk	Residual Risk
Replication of video or audio stream.	Footage of the teacher or other students in the class recorded and posted online. Potential embarrassment to a teacher. Photos/ videos of pupils faces online without consent.	• The AV1 Terms & Conditions of use, which the user or their legal guardian must accept prior to use, strictly forbid this behaviour • The app does not allow screen recordings. The recording would have to be done with another device such as a phone. • The app will penalise a user if a screenshot is taken. They will have to contact No Isolation to gain access to their AV1 again after attempting a screenshot. • There are easier ways to record in a classroom than via an AV1. • A sick child and their family are unlikely to want to ruin their chance of using AV1 by breaking terms. • If a child/parent were to upload a recording of the class, the consequence of this data breach lies with the family and not the school.	• Permit the use of AV1 for those whose parents you trust will respect the Terms & Conditions. • Educate the child and parents on the importance of adhering to the Terms & Conditions, and the consequences of not adhering. • Where possible, enforce the use of headphones when streaming through AV1. • Consider buying a privacy shield for the tablet. This is a thin layer that you can stick on your tablet to prevent viewing the content from any angle other than directly straight on. • Consider setting up Apple's "Guided Access" if using the AV1 app on an iPad, which limits the use of certain apps e.g. Facebook, so that a screenshot could not be immediately uploaded. • If a recording is uploaded online, a No Isolation lawyer will send a "Cease & Desist" letter to the social media company and the individual who made the post. This letter threatens legal action unless the post is taken down. In addition, the school should ask the person responsible to take the media down, and/or report the post to the social media company. You should follow standard school procedures as if the recording had been made with a mobile phone.	Minimal

2

Activity	Risk	Considerations	Control measures/ possible actions to reduce risk	Residual Risk
AV1 user hearing or seeing things that they should not have.	AV1 user over-hearing confidential conversations, or AV1 being taken to inappropriate locations.	• AV1 can be switched off using the button on its back. Whilst switched off the user cannot log into AV1. The AV1 can charge whilst turned off. • You can clearly see when someone is connected to AV1 as the LED eyes will be lit up.	• Get into a habit of turning off the AV1 and plugging it in to charge at the end of each school day. • If the staff room is a place where confidential conversations are likely to happen then you might wish to charge/store your AV1 in another room. • Agree a set timetable with the AV1 user, so that they log in at set times only. • Implement a buddy system with trusted students who are responsible for getting the AV1 to the right room and returning it when class has finished. • If the child overhears something they shouldn't, immediately contact the child and their family and talk about the importance of keeping that confidential, and making sure to log out immediately if it happens again.	Minimal

3

Activity	Risk	Considerations	Control measures/ possible actions to reduce risk	Residual Risk
The AV1 user being bullied by other children in the class.	The children in the class could say harmful things that the AV1 user at home could hear.	• The class is likely to miss their peer, and would not want to hurt their feelings. • AV1 is generally perceived by children and young people as "cool", and therefore they do not find reason to bully their sick friend for using it. • The class cannot see the child at home. There is no chance of accidentally seeing the child in their pajamas, or in any other compromised situation. • AV1 can be switched off using the button on its back if the teacher hears harmful comments being said during class.	• Educating the school about AV1 is crucial prior to using it for the first time. Make use of No Isolation's lesson plan and template letters for parents. Do not allow the AV1 user to have their first class with AV1 until you are confident that everyone will be respectful. • If the AV1 user has a history of being bullied, make a careful consideration about whether AV1 is the best tool for this child. • If bullying occurs, follow standard school bullying procedure. If bullying persists, you may reason that it is better to find another solution for that child's education access, such as home tuition or alternative provision.	Minimal

4

Activity	Risk	Considerations	Control measures/ possible actions to reduce risk	Residual Risk
The class hears something from home or hospital that they should not.	The children in class and the teacher might hear a doctors consultation or a private conversation amongst the family at home.	• The AV1 app has a 'Mute' feature. When pressed, any sound at the AV1 users end will not be transmitted through the tablet and out the AV1 speaker. • The child is not likely to stream through their AV1 during an important or personal event.	• Educate the child about the 'Mute' feature prior to letting them use AV1 in class. Make use of No Isolation's AV1 'User Guide' for this. • Ensure that the parents of the AV1 user understand how the technology works in terms of transmitting sound into the classroom. • Recommend that the child only uses their AV1 when in a quiet room by themselves, and unlikely to be disrupted. • If the class does hear something that they shouldn't, turn off the AV1 as quickly as possible, and explain to the class the importance of protecting that young persons privacy by not discussing the matter outside of the classroom.	Minimal

5

Activity	Risk	Considerations	Control measures/ possible actions to reduce risk	Residual Risk
The AV1 will be used by someone other than the intended user.	A parent, sibling, neighbour, or stranger may log into the AV1 app, and the class will not be aware of this.	• To activate AV1 for the first time, the user must enter a single-use 8-digit keyword, which syncs their device to a particular AV1. This keyword will be given to the customer, who is responsible for making sure it safely reaches the intended AV1 user. • The AV1 Terms & Conditions of use, which the user or their legal guardian must accept prior to use, state that only the child/intended user will use the AV1 app. • The AV1 app requires the user to input their 4-digit pin code every time they use AV1. This code is secret only to the child. • There is little cause for anyone other than the intended user to want to see and hear what is happening in the class. A classroom is an innocent place that most onlookers would find no interest in observing.	• Educate the child their parents/ guardians about the terms of use. Make use of the AV1 'User Guide', as well as the template information letters for parents. • Enforce that it is only the child/ intended user who should know the 4-digit pin code. • If the child is young, or has a health need that means an adult is often or always present in the same room as the child, we recommend that you make your own terms and conditions with the family, adding a clause concerning which named adults are allowed to be in the room when AV1 is being used. Templates for this are available from No Isolation. • If you suspect that someone other than the intended user is accessing the AV1, we recommend asking a question to the AV1. If there is no response, you may wish to turn the AV1 off. If you are persistently concerned you can contact No Isolation for a new keyword to re-sync the child's device, or the AV1 can be deactivated.	Minimal

6

Activity	Risk	Considerations	Control measures/ possible actions to reduce risk	Residual Risk
The AV1 stream will be hacked by external parties, or it will be viewed by No Isolation.	The livestream will be viewed and potentially recorded on another device, without the knowledge of those in the class,	• AV1 streams using WebRTC, meaning all media sent is end-to-end encrypted, enacted through standardised and well-known encryption protocols (SRTP/ DTLS). Where possible the stream is peer-to-peer between the user and AV1, meaning the stream will not go through any servers. When networks do not allow peer-to-peer the stream is relayed through Twilio, a secure and industry leading provider for connectivity. Since the media is end-to-end encrypted neither Twilio nor No Isolation can see the stream. • Hacking is incredibly difficult. If someone goes to the effort of hacking, it is more likely that they will hack something more worthwhile, such as an online bank account.	• If you suspect that someone has hacked AV1, notify No Isolation immediately. • No Isolation monitor all attempts to hack our servers, and have never been hacked. • In the very rare situation that No Isolation's servers are hacked, No Isolation will report it to the authorities within 72 hours, as per internal protocol, even if the issue is solved before 72 hours has passed.	Minimal

Signed: .....

Role: .....

Date: .....

Signed: .....

Role: .....

Date: .....