
Ericsson Case Study 1: Connect To Learn

Since 2010, Ericsson has been the lead technology partner in Connect To Learn, an initiative with Columbia University's Earth Institute and Millennium Promise. Connect To Learn has supported UNESCO's Education for All goals, by deploying mobile broadband and cloud solutions, combined with hands-on training in Information and Communication Technology (ICT), to schools in 14 countries.

[Connect to Learn](#)

Outcomes:

Innovative educational platforms that promote learning, creative thinking and problem solving, and

Promotion of digital literacy, capacity building and ICT skills

Ericsson Case Study 2: Child-Friendly Computing Concept

Ericsson is working together with Lund University Innovation System (LUIS AB) within the Connect To Learn project in developing the basis of a child-friendly computing concept based on the United Nations Convention on the Rights of the Child.

The aim is to create a student friendly computing environment for schools, suitable for the emerging markets. The whole development process has a child rights-based approach. Instead of trying to produce an affordable version of the typical western PC the LUIS solution starts from a deep understanding of cultural, legal, technical and business challenges in emerging markets when developing a custom designed computing solution. It is designed to bridge digital divides while taking into consideration the Convention of the Rights of the Child, Education for All and other internationally agreed instruments.

Outcomes:

Creating a safer and age-appropriate online environment (technical measures to prevent underage access and exposure to inappropriate content, terms and conditions, privacy controls, reporting tools, marketing and advertising), and

Educating children, parents and teachers about children's safety and their responsible use of information and communication technologies

Ericsson Case Study 3: company-wide initiative taking Action Against CSA Content

Since 2011, Ericsson has taken action against child sexual abuse (CSA) by detecting and eliminating CSA content, identified by law enforcement authorities, found on Ericsson corporate IT resources. The idea to detect and eliminate CSA content from Ericsson IT resources started to take form when Ericsson learned about the emerging technological possibilities to address this problem. The feasibility of introducing this type of program – the first of its kind in a company as large as Ericsson – was carefully studied from all angles: legal, technical, union, employee and employment. The feasibility was confirmed and our company-wide Action Against CSA Content initiative was started.

The key principles considered when developing this program are listed below:

Prior to program deployment, ensure

- Governance for the program is established to identify and manage risks associated with this type of program, including legal, security, labor/employer, communication and brand risks and opportunities
- All legal re-requisites to deploy CSA detection technology in the organization are identified and satisfied for each country; these can include communication requirements, personal consent, or other requirements; approval to deploy is given one a country-by-country basis.
- Roles and responsibilities are clearly defined to handle any CSA case that may arise

- The program is fully documented; information about the program is communicated on both the internally-facing and externally-facing webpages
- A principle is established and communicated that participation in the management and operation of this program is fully voluntary; although this type of program would ensure that CSA content is never shown or described to those governing this program or managing CSA incidents, the topic itself is disturbing. As such, participation can be re-assigned at any time without question; debriefing possibilities are made known to all participants

Considerations when developing a CSA incident handling process:

- Take every measure to ensure that CSA incidents are handled professionally, consistently and accurately in accordance with relevant legal requirements and considerations.
- Safeguard the company and the individuals involved in handling CSA incidents from being accused of planting, distributing or otherwise taking part in CSA imagery.
- Ensure the process for handling CSA incidents can assure the integrity of the material necessary for confirming the details of the CSAI, possibly in a court of law.

