

Uttaran

Digital guideline or cyber security guideline

Community Mobilization

Poverty Eradication

Environmental Justice

Contact Information:

Head office: Flat # B1, House # 32, Road # 10/A, Dhanmondi, Dhaka 1209

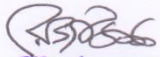
Regional Office: Mobarakpur, Tala, Satkhira- 9420

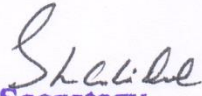
Email: uttaran.dhaka@gmail.com

Website: www.uttaran.net, Contact no: +880-1711828305, +880255000691

Facebook: www.facebook.com/org.uttaran, Twitter: @Org.Uttaran, Instagram: org.uttaran

01	Date: 02 November 2020	
	Approved by on behalf of executive board	Shahidul Islam Sarder Md. Rezaul Karim Director Chairman
	Recommended by	Haridas Malakar, Coordinator (Accounts and Finance)


Chairman
UTTARAN
 House No-32, (1st Floor) Road No-10/A
 Dhanmondi R/A, Dhaka-1209, Bangladesh


Secretary
UTTARAN
 House No-32, (1st Floor) Road No-10/A
 Dhanmondi R/A, Dhaka-1209, Bangladesh

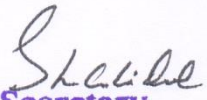
Introduction

Uttaran is one of the largest development organizations in the south-western region of Bangladesh. Uttaran now deals a varied number of projects, including improving the rights of life and livelihoods of the poor people, protecting human rights, women empowerment, access of the landless on government lands and public service, water management and protecting river navigability, providing legal support, battling challenges of climate change, disaster management, primary health education, education service, water and sanitation and health rules, microcredit activities, food security and forming a republican society, sustainable agriculture, landscape and many others, are being implemented in Bangladesh. Some of the tasks have made it more popular among the people and the notable tasks are the access of the landless on demesne, achieving rights of the untouchable peoples, women empowerment, educational activities, TRM for water clogging and protecting human rights.

As the global world is changing rapidly so are our activities. Amidst the Coronavirus Pandemic Uttaran had to take even more drastic measures to ensure that we reach to our participants with no harm approach. Thus a lot of our activities were conducted online through various social media platforms. In this regard Uttaran understands that these platforms can face various threats from online illegal activities and cybercrimes. Uttaran is committed to protecting the cyber security of the information which anybody shares with organization's websites, pages, e-mails etc.

In addition the COVID-19 emergency has changed how children and adolescents around the globe are being educated, with distance schooling and studying online becoming the new normality for school children almost everywhere. While children, teachers and parents started necessary adaptation, this novelty suddenly unveiled at unprecedented scale, new equity gaps, risks and vulnerabilities. Uttaran has undertaken various development projects which included adolescents and youths. Furthermore Uttaran is trying to incorporate underprivileged children into digital education by introducing digital devices. The traditional training or schooling experience is suddenly getting reshaped with technology, internet, screen and e-platform driven learning as a substitute for the classrooms and hardcover books. While many youths and children perhaps got excited with the idea to be 'online' more often, their parents, caregivers and teachers found themselves mostly unprepared neither for digital literacy support nor for guidance to online safety. Longer hours online connected through digital devices both for entertainment and for education purposes, means increased exposure to online risks for children, adolescents, and youths. Thus this policy was adopted to ensure all of Uttaran's digital activities remains safe for all of its stakeholders, especially children, adolescents and youths. The guidance note will prove beneficial to Uttaran's training facilitators, educational authorities, development or philanthropic partners, NGOs as well as ICT industry actors that are engaged in distribution of digital devices for children.


Chairman
UTTARAN
House No-32, (1st Floor) Road No-10/A
Dhanmondi R/A, Dhaka-1209, Bangladesh


Secretary
UTTARAN
House No-32, (1st Floor) Road No-10/A
Dhanmondi R/A, Dhaka-1209, Bangladesh

The sites used by the organization are Facebook, Twitter, Instagram, LinkedIn.

Uttaran's digital platforms:

Hotline: +88-01743116354

e-mail: uttaran.dhaka@gmail.com

Web: www.uttaran.net

Facebook: www.facebook.com/org.uttaran

Instagram: org.uttaran

Twitter: @org.uttaran

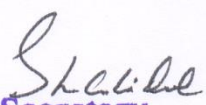
Overview:

	Commercial	Aggressive	Sexual	Values
Content – child as recipient	Adverts Spam Sponsorship Personal information	Violent/ hateful content	Pornographic or unwelcome sexual content	Bias Racist Misleading information or advice
Contact – child as participant	Tracking Harvesting Personal information	Being bullied Being harassed Being stalked	Meeting strangers Being groomed	Self harm Unwelcome persuasions
Conduct – child as actor	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading information or advice

All of Uttaran's programmes and projects should follow and protect its vulnerable population from:

1) **Cyberbullying:** is probably the biggest risk that children and young people face in the developed world but it is also on the rise in countries such as China, India and Bangladesh. A study in India suggests that 65% of surveyed school students have been victims of mobile phone bullying and that 60% have been involved in bullying others. Data from Thailand indicates that 35% of seven-11 year olds have had exposure to web sites displaying pornographic material. Of older respondents 71%


Chairman
UTTARAN
House No-32, (1st Floor) Road No-10/A
Dhanmondi R/A, Dhaka-1209, Bangladesh


Secretary
UTTARAN
House No-32, (1st Floor) Road No-10/A
Dhanmondi R/A, Dhaka-1209, Bangladesh

have visited porn sites voluntarily. A particularly serious risk that has been identified in developing countries is exploitation of young people via social media from donors, especially where there is a one-to-one sponsorship arrangement. Keeping Children Safe has provided detailed guidance around best practice for managing communication using social media with donors and sponsor children. Social media offers new opportunities for contact by donors and abuse can take place online – via web cam for example – and can also lead to offline abuse:

- Donors can make unsolicited contact via social media, tracing children and their families.
- Sponsored children can receive unwanted and inappropriate images/content.
- Sponsored children could experience live/real time abuse – particularly sexual abuse via social media.
- Children may be subjected to an increased network of adults who wish to exploit them. At present there is little evidence that donors are abusing children and young people via social media but NGOs have recognised that where there is one-to-one sponsorship of a child there is an imbalance of power and therefore an opportunity for exploitation.

2) **Social Media:** During planning projects involving the use of social media and digital technology, the project coordinator or programme head need to understand the environment in which they are working in order to reduce the risks to young people. The PIES model, which has been tried and tested in the UK and elsewhere, is an effective tool for reducing risks. (Becta, 2009) The PIES model centres around four core areas: Policies and practices; Infrastructure; Education; and Standards

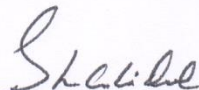
Policies and practices: refer to the types of e-safety policies and procedures that organisations need to have in place. For instance, a policy should describe the acceptable use of technology and outline the sanctions should this be breached.

Infrastructure: The technological infrastructure that Uttaran uses plays a key role in protecting children and young people. Uttaran need to consider which technical solutions can be implemented to ensure safety.

Education: Uttaran must ensure that staff, volunteers, children and young people, as well as the wider community, receive the most appropriate education and training in the proper use of ICT and social media.

Standards: All the above need to be constantly monitored and reviewed in order to protect children and young people. Ongoing reviews of the ‘standards’ of the approach are essential and need to be carried out across different levels, including internal child safeguarding, social media standards or guidelines, external laws or governance arrangements, or inspection approaches.


Chairman
UTTARAN
House No-32, (1st Floor) Road No-10/A
Dhanmondi R/A, Dhaka-1209, Bangladesh


Secretary
UTTARAN
House No-32, (1st Floor) Road No-10/A
Dhanmondi R/A, Dhaka-1209, Bangladesh

Putting the PIES model into practice

The checklist below can be used to implement the PIES model:

- 1 Understand the context and risks: research the context in which Uttaran will use social media and which legal instruments support safeguarding. Carry out an audit with key stakeholders to establish levels of use, risk and awareness. Use this to shape your approach.
- 2 Policies and practices: Examine and assess existing policies such as safeguarding and child protection policies, reporting, and escalation policies and processes. Consider whether existing policies cover the relevant aspects. If not, develop new policies, particularly relating to social media and acceptable use. Involve stakeholders to do this.
- 3 Infrastructure and technology: look at the most appropriate technology and/or services to use. Set up technical solutions that will help to lessen and manage risks to young people, staff and volunteers.
- 4 Education and training: consider educational approaches for all involved – staff, children and young people, volunteers and parents and stakeholders.
- 5 Standards: use internal and external feedback to continually inform and develop the approach.

Research the context

When planning any project that incorporates social media, it is important to take into account the legal and cultural situation in the area where the project will take place.

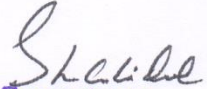
National laws relating to online abuse must be followed in order to safeguard children and young people.

Keeping children safe online A guide to an organizational approach

Local cultural and social issues may affect risk, access and education. These need to be taken into account when planning strategy. Local laws too may affect the way in which e-safety strategies can be implemented.

Conduct a risk assessment Before planning projects using social media, the programme head or safeguarding focal must carry out a risk assessment or audit in order to review and understand the safety risks within the context in which you are working. This needs to take place before implementing any social media strategy. The audit will help you understand the type of approach that needs to be taken and the issues that need to be tackled


Chairman
UTTARAN
House No-32, (1st Floor) Road No-10/A
Dhanmondi R/A, Dhaka-1209, Bangladesh

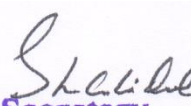

Secretary
UTTARAN
House No-32, (1st Floor) Road No-10/A
Dhanmondi R/A, Dhaka-1209, Bangladesh

Sexting: Teenagers are using mobile phones to produce clips featuring boys and girls engaged in sexually explicit behavior, highlighting the role of mobile phones in the distribution of such materials in the developing world. Sexting is also an increasing phenomenon in all over South Asia, using messenger app or just mobile messaging. Increasingly photos were reinforcing offline gender based relationships; that is photos were used as “currency” and status.

Procurement phase: In order to minimize situations in which children/adolescent/youth might encounter harmful behaviour and content, safety features need to be built into technological products or services from the outset. If you or your company are planning to acquire digital devices that will be used by children, ensure that contracts with ICT suppliers envisage safety and security considerations in all digital devices, including:

- a. **Manual for the use of the device** translated in Bangla;
- b. **Protective cases (dustproof, shockproof) and protective glass and safe headphones** for children/adolescent receiving the digital devices should be purchased together with the digital devices;
- c. **The dimension of the screen** of the digital device should be at least 7-inch for a safe experience;
- d. Digital devices should have **chargers and power adaptor for 220 volts** (as per Albanian households use);
- e. **Pre-installed educational and collaboration applications** (as per educational authorities’ guidance and usage) grouped in one folder or with shortcuts on the desktop of the digital device. Some examples include:
 - i. Educational e-learning platforms: School, collage etc;
 - ii. Digital learning management systems: Zoom meeting, Google Classroom
 - iii. Collaboration applications: Zoom, Skype, What’s App.
- f. Digital devices should have **2 modalities/accounts** already installed and running: one password protected account for parents as Administrator and one for the child. Through the parental account, the parent should be able to manage different safety features of the child’s account: how much time they can use the digital device per day, what they can and cannot watch/play, manage their installed apps, etc. When it comes to younger children, those features could include parental controls, firewalls, and apps designed specifically for children. Other measures could include content rating and classification so that children do not have unwanted exposure to extreme violence and pornography; age verification tools; tools for reporting misuse and abuse; as well as removal and blocking of illegal content such as child abuse material.
- g. Ensure that **Antiviruses** are provided across all systems and devices, including installation, at least 3-year guarantee, licences and related keys. The Antivirus should provide total protection, including comprehensive protection for the systems and should be able to guard against the latest threats – block viruses, malware, ransomware, spyware, unwanted programs, etc.


Chairman
UTTARAN
House No-32, (1st Floor) Road No-10/A
Dhanmondi R/A, Dhaka-1209, Bangladesh


Secretary
UTTARAN
House No-32, (1st Floor) Road No-10/A
Dhanmondi R/A, Dhaka-1209, Bangladesh

h. Ensure **maintenance of device** and support to families for at least 2 years from delivery to beneficiary (either with a contact number for remote support or through a face to face support expert).

3) **Internet connectivity:** To ensure effective internet access for vulnerable children, organisations or institutions purchasing and delivering digital devices should consider supporting families with internet connectivity packages such as:

i. **Pre-registered SIM cards** in case the digital device is working with 3G-4G (e.g. tablets). SIM cards should be automatically set for only data (ideally 5GB data for videos, uploading and remote learning), while the telephone modality should be disabled to ensure families are not charged with additional costs;

ii. **Filtered internet connection** from child abuse materials and adult pornography (for both broadband cabled internet and Wi-Fi). A filtered internet connection reassures parents and caregivers that the internet children are using blocks access to adult pornography and all the blacklisted child sexual abuse web contents.

Parent Control Guide: Upon delivery of products, ensure that dedicated Parental Control Guides are provided to parents, caregivers and teachers in Albanian language, including easily understandable options for them to download and monitor.

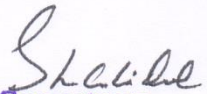
The guide can be in printed booklets or through audio-visual materials and should contain the minimum information for parents on how to:

- open email addresses;
- block websites and filtering illegal and harmful content;
- set limits and monitor the activities of children
- manage screen time tools;
- disable location tracking;
- connect all children's digital devices to parent's accounts, etc.

Accessibility: When providing digital devices for children with disabilities ensure their compliance with the standards of accessibility as per best practice in assistive technologies.

Uttaran is constantly becoming more and more intertwined with online technology. Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as


Chairman
UTTARAN
House No-32, (1st Floor) Road No-10/A
Dhanmondi R/A, Dhaka-1209, Bangladesh


Secretary
UTTARAN
House No-32, (1st Floor) Road No-10/A
Dhanmondi R/A, Dhaka-1209, Bangladesh

information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories. Network security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

Uttaran stores it's all type of data electronically and even the laws of the state are stored in a digital form. Another example of how dependent organizations are on the internet, are groups that have to do with the protection of human rights who need to use specific programs for their communications. Their exclusive usage of digital technology to store and send sensitive information makes cyber security a top priority for Uttaran. Information security protects the integrity and privacy of data in storage. Application security focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Operational security includes the processes and decisions for handling and protecting data assets.

With the scale of the cyber threat set to continue to rise, the International Data Corporation predicts that worldwide spending on cyber-security solutions. Our Governments across the globe have responded to the rising cyber threat with guidance to help organizations implement effective cyber-security practices.

Disaster recovery and business continuity define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event.

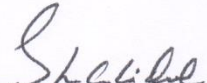
Types of cyber threats

The threats countered by cyber-security are:

1. Cybercrime includes single actors or groups targeting systems for financial gain or to cause disruption.
2. Cyber-attack often involves politically motivated information gathering.
3. Cyber terrorism is intended to undermine electronic systems to cause panic or fear.

So, how do malicious actors gain control of computer systems? Here are some common methods used to threaten cyber-security:


Chairman
UTTARAN
House No-32, (1st Floor) Road No-10/A
Dhanmondi R/A, Dhaka-1209, Bangladesh


Secretary
UTTARAN
House No-32, (1st Floor) Road No-10/A
Dhanmondi R/A, Dhaka-1209, Bangladesh

Malware

Malware means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user's computer. Often spread via an unsolicited email attachment or legitimate-looking download, malware may be used by cybercriminals to make money or in politically motivated cyber-attacks.

There are a number of different types of malware, including:

- **Virus:** A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.
- **Trojans:** A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.
- **Spyware:** A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.
- **Ransomware:** Malware which locks down a user's files and data, with the threat of erasing it unless a ransom is paid.
- **Adware:** Advertising software which can be used to spread malware.
- **Botnets:** Networks of malware infected computers which cybercriminals use to perform tasks online without the user's permission.

SQL injection

How can Uttaran guard against cyber threats? Here are the top cyber safety tips:

1. **Update your software and operating system:** This means you benefit from the latest security patches.
2. **Use anti-virus software:** Security solutions like Kaspersky Total Security will detect and removes threats. Keep your software updated for the best level of protection.
3. **Use strong passwords:** Ensure your passwords are not easily guessable.
4. **Do not open email attachments from unknown senders:** These could be infected with malware.
5. **Do not click on links in emails from unknown senders or unfamiliar websites:** This is a common way that malware is spread.
6. **Avoid using unsecure WiFi networks in public places:** Unsecure networks leave you vulnerable to man-in-the-middle attacks.

