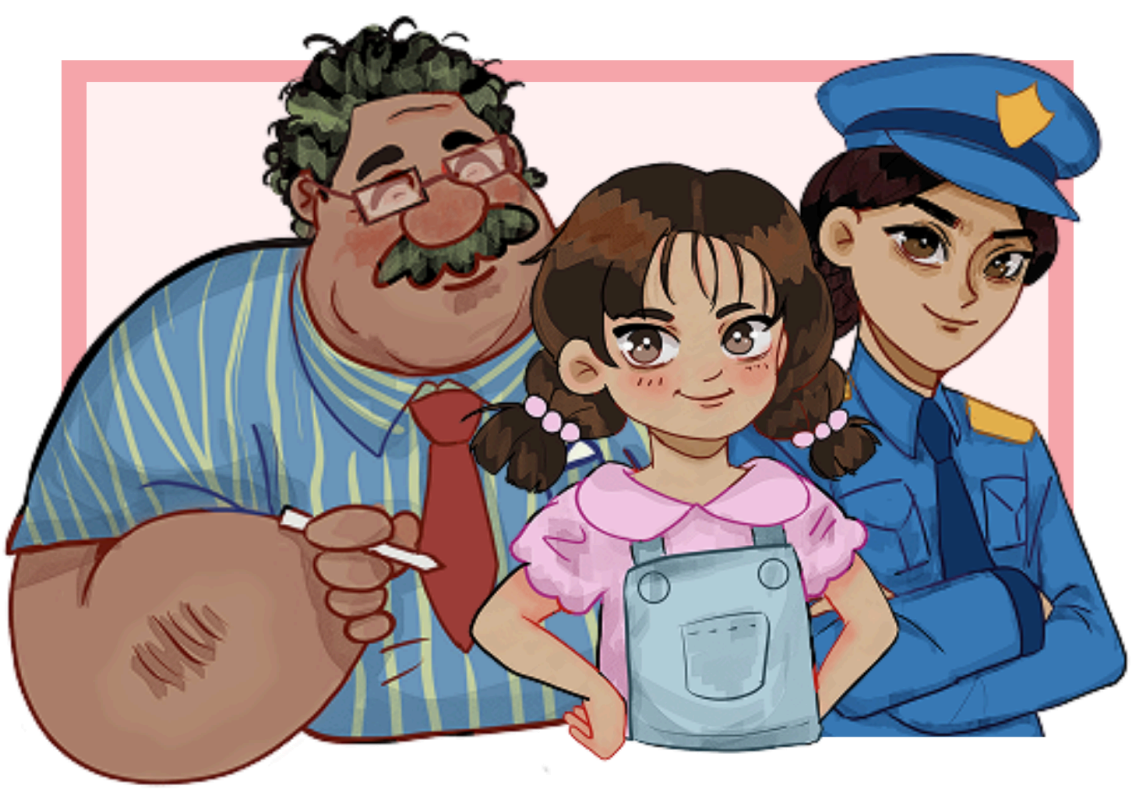
एकाइ १०

अनलाइन दुर्व्यवहार प्रतिक्रिया (Reaction)



Supported By:

ASML Foundation

Alternatives 4 children

अनलाइन दुर्व्यवहार प्रतिक्रिया (Reaction)

सिकाइका लक्ष्यहरू

यस पाठ एकाइको अन्त्यसम्ममा विद्यार्थीहरू निम्न कुराहरू गर्न सक्षम हुनेछन् :

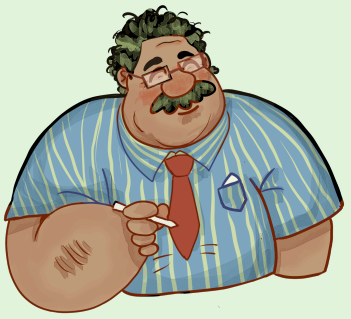
- अनलाइन उत्पीडन र दुर्व्यवहारका सामान्य र हानिकारक रूपहरू, जसमा फिसिङ्ग (phishing) र डिजिटल दुर्व्यवहार समावेश छन्, परिभाषित र पहिचान गर्न ।
- सुरक्षित पोस्ट वा शेयर गर्ने सीमाहरू स्थापना गर्न व्यक्तिगत (personal) र निजी (private) जानकारी बीचको भिन्नता बुझ्न ।
- डिजिटल दुर्व्यवहारका चेतावनी संकेतहरू पहिचान गर्ने र यसले मानसिक तथा सामाजिक कल्याणमा पार्ने गम्भीर प्रभाव बुझ्न।
- डिजिटल दुर्व्यवहारलाई सुरक्षित रूपमा प्रतिक्रिया दिन र नेपालमा उपलब्ध कानुनी प्रणालीहरू प्रयोग गरेर यसलाई रिपोर्ट गर्नका लागि चरणवद्ध प्रक्रियाहरू सिक्न ।
- सहयोगी, सम्मानजनक र सुरक्षित अनलाइन समुदायहरू निर्माणका लागि योगदान गर्न ।

परिचय: इन्टरनेटको दुई पाटा - जडान र जोखिम

इन्टरनेट एउटा अचम्मको प्लेटफर्म होः यसले तपाईंलाई संसारको बारेमा सिक्न, आफ्नो रचनात्मकता देखाउन र विदेशमा बसिरहेका साथीहरू र परिवारसँग जोडिन दिन्छ । तर कुनै पनि शक्तिशाली उपकरणजस्तै यसको पनि दुरुपयोग हुन सक्छ ।

जब मानिसहरूले जानीजानी डर वा हानि पुर्याउन प्रविधिको प्रयोग गर्छन्, तब हामी अनलाइन दुर्व्यवहार (Online Abuse) को सामना गर्छौं ।

नेपालमा धेरै युवाहरू डिजिटल माध्यममा पहुँच बढाउँदै छन्, जसले उनीहरूलाई अनलाइन जोखिमहरू बुझ्न र सुरक्षित तरिकाले प्रतिक्रिया दिन सक्षम हुन आवश्यक बनाएको छ।



शिक्षक विकास
(Teacher Bikash)

"नमस्ते! हामी आज तपाईंको भविष्य सुरक्षित बनाउन सहयोग गर्ने महत्त्वपूर्ण सीपहरू सिक्नेछौँ । याद राख्नुहोस्—तपाईंको डिजिटल हित (Digital well-being) तपाईंको शारीरिक सुरक्षाजत्तिकै महत्त्वपूर्ण छ। आज हामी के पोस्ट वा शेयर गर्न सुरक्षित छ र के कुराले अनावश्यक जोखिम निम्त्याउन सक्छ भन्ने कुरा छुट्याउन सिक्नेछौं।"

जानकारीको सिमाना : व्यक्तिगत VS निजी

आफूलाई सुरक्षित राख्न, तपाईंले के सुरक्षित गर्न चाहनुहुन्छ भन्ने स्पष्ट रूपमा बुझ्न आवश्यक छ। व्यक्तिगत र निजी जानकारीबीच स्पष्ट सीमा निर्धारण गर्नु नै डिजिटल सुरक्षाको पहिलो कदम हो।

जानकारीको प्रकार	यसको अर्थ (What It Means)	तपाईंको नियन्त्रण (Your Control)
व्यक्तिगत (Personal)	यो जानकारी तपाईंको पहिचानको लागि आवश्यक छ र सार्वजनिक रूपमा प्रयोग गर्न सुरक्षित छ ।	**उच्च :** सामान्यतः तपाईं सार्वजनिक रूपमा शेयर गर्न सुरक्षित हुनुहुन्छ ।
निजी (Private)	यो जानकारी तपाईंको पहिचान वा सुरक्षालाई हानी पुर्याउन प्रयोग गर्न सकिन्छ ।	**निम्न :** यो जानकारी कहिल्यै शेयर नगर्नुहोस् ।

थप सामग्री : 👉 Personal vs Private Information

आफ्नो डिजिटल पहिचानको सुरक्षा गर्नु

व्यक्तिगत जानकारी (पोस्ट वा शेयर गर्न सुरक्षित - Safe to Share)	निजी जानकारी (पोस्ट वा शेयर गर्न सुरक्षित छैन - Not Safe to Share)
तपाईंको पहिलो नाम वा उपनाम (nickname) ।	तपाईंको फोन नम्बर ।
तपाईंको मनपर्ने रुचि।	तपाईंको प्रमाणहरू (credentials) जस्तै पासवर्ड, बैंक नम्बरहरू ।
तपाईंको सहर वा राज्यको नाम ।	तपाईंको पूरा ठेगाना (जस्तै सडक, घर नम्बर)
तपाईंको एक सार्वजनिक फोटो (यदि तपाईंले पोस्ट गर्न छनौट गर्नुहुन्छ भने) ।	तपाईंको निजी फोटो र भिडियोहरू ।

पोस्ट वा शेयर गर्ने नियम : निजी जानकारीलाई तपाईंको घरको साँचो वा नगद जस्तै व्यवहार गर्नुहोस् : तपाईंले यसलाई आफूले पूर्ण रूपमा विश्वास गर्ने मानिसहरूसँग मात्र पोस्ट वा शेयर गर्नुहुन्छ र यसलाई सार्वजनिक टिप्पणी वा सन्देशहरूमा कहिल्यै नछोड्नुहोस् ।

अनलाइन दुर्व्यवहार परिभाषित गर्ने

अनलाइन दुर्व्यवहार तब हुन्छ, जब कसैले सन्देश, पोस्ट, टिप्पणी, इमेल वा अन्य डिजिटल माध्यमहरूको बारम्बार प्रयोग गरेर कुनै व्यक्तिलाई हानी, डर वा अपमानित गर्न खोज्छ। यसमा हानी पुऱ्याउने उद्देश्य (intent) र पीडितमा पर्ने प्रभावले नै अपराध परिभाषित गर्छ। अनलाइन दुर्व्यवहार एकै प्रकारको हुँदैन । यहाँ केही सामान्य रूपहरू छन् :

प्रकार (Type)	यसको अर्थ (What It Means)	उदाहरण (Example) र तपाईंको कार्य (Your Action)
साइबर बुलिङ (Cyber-bullying)	डिजिटल माध्यमबाट जानीजानी र बारम्बार हुने हानी ।	**उदाहरण :** कसैको हाजिरी वा अनुहारको बारेमा नकारात्मक टिप्पणीहरू पोस्ट वा शेयर गर्नु । **तपाईंको कार्य :** तुरुन्तै ब्लक र रिपोर्ट गर्नुहोस् ।
ट्रोलिङ (Trolling)	विवाद वा नकारात्मक प्रतिक्रिया सिर्जना गर्न जानीजानी उत्तेजक (provocative) वा अपमानजनक टिप्पणीहरू गर्नु ।	**उदाहरण :** कसैको पोस्टमा रिसको प्रतिक्रिया दिन वा केवल ध्यान आकर्षित गर्न अपमानजनक शब्द प्रयोग गर्नु । **तपाईंको कार्य :** बेवास्ता गर्नुहोस् ।
सङ्गठित ट्रोलिङ (Organized Trolling)	ट्रोलिङको अधिक हानिकारक रूप जहाँ एक व्यक्ति वा समूहले अर्कोलाई सङ्गठित रूपमा निशाना बनाउँछ ।	**उदाहरण :** एक समूहले राजनीतिक पोस्ट गर्ने एक शिक्षकको विरुद्धमा हजारौं नक्कली खाताहरू प्रयोग गरेर एकैचोटि अपमानजनक टिप्पणीहरू पठाउनु । **तपाईंको कार्य :** प्रमाण सङ्कलन गर्नुहोस् (Screenshot) र कानुनी रूपमा रिपोर्ट गर्नुहोस् ।
डोक्सिङ (Doxing)	बदला लिने उद्देश्यले अनलाइनमा कसैको निजी जानकारी (घरको ठेगाना, फोन नम्बर) पोस्ट वा शेयर गर्नु ।	**तपाईंको कार्य :**तुरुन्तै प्लेटफर्ममा रिपोर्ट गर्नुहोस् र कानुनी कारबाही गर्न सक्नुहुन्छ ।

विशेष ध्यान दिनुहोस् : दुर्व्यवहार र साइबर अपराध

फिसिङ्ग (Phishing) जस्ता साइबर अपराध (Cyber-crime) लाई अनलाइन दुर्व्यवहारमा समावेश गरिन्छ किनभने तिनीहरू पनि डर र छल (Deception) प्रयोग गरेर हानी पुर्याउन खोज्छन् ।

इन्स्पेक्टर सीता
(Inspector Sita)

"ध्यान दिएर सुन्नुहोस् : अनलाइन उत्पीडन नेपालमा गम्भीर अपराध हो । इलेक्ट्रोनिक कारोबार ऐन (ETA) २०६३ (2008) को दफा ४७ ले तपाईंलाई सहमतिबिना निजी जानकारी पोस्ट वा शेयर गर्ने, मानहानी गर्ने वा कसैको खाता ह्याक गर्ने कार्यलाई आपराधिक ठहर्याएर सुरक्षा दिन्छ । स्क्रिन पछाडि लुक्दा कानुनबाट बच्न सकिन्छ भन्ने नसोच्नुहोस् । कानुनले डिजिटल अपराधहरूलाई गम्भीर रूपमा लिन्छ किनभने हानी वास्तविक हुन्छ ।"

यदि कुनै कुरा तपाईंलाई ठीक लागेन भने, सम्भवतः त्यो गलत नै हुन सक्छ । यसलाई सजग दृष्टिले हेर्नुहोस र विश्वासयोग्य व्यक्तिसँग छलफल गर्नुहोस् ।

संकेतहरू चिन्ने र सुरक्षित रूपमा प्रतिक्रिया दिने

दुर्व्यवहार सधैं ठूला वा प्रत्यक्ष घटनाबाट मात्र सुरु हुँदैन। धेरैजसो अवस्थामा यो साना–साना व्यवहार वा संकेतबाट सुरु हुन्छ, जसले कसैलाई असहज, दबाबमा परेको वा नियन्त्रणमा राखिएको जस्तो अनुभूति गराउन सक्छ। यदि कुनै व्यवहार तपाईंलाई अस्वाभाविक वा ठीक नलागेमा, त्यसलाई बेवास्ता नगर्नुहोस्—गम्भीर रूपमा लिनुहोस् र विश्वास गर्न सकिने व्यक्तिसँग खुला रूपमा कुरा गर्नुहोस्।

तपाई वा तपाईको साथी अनलाइन दुर्व्यवहारको सामना गरिरहनुभएको हुन सक्ने सङ्केतहरू :

भावनात्मक परिवर्तनहरू :

सामाजिक सञ्जाल खोल्नुअघि वा सन्देश हेर्नुअघि अचानक डर, चिन्ता, वा मन भारी भएको महसुस हुनु ।

नियन्त्रण गुमेको महसुस :

स्पष्ट रूपमा रोक्न भनेपछि वा ब्लक गरिसकेपछि पनि कसैले तपाईंलाई बारम्बार त्याग गरिरहनु, सन्देश पठाइरहनु, वा पोस्टमा टिप्पणी गरिरहनु ।

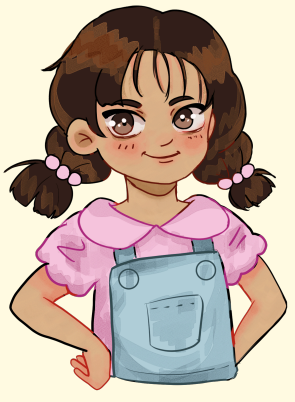
निजी कुरामा समस्या आउनु :

तपाईको अनुमति बिना तपाईका निजी जानकारी, तस्बिरहरू वा सन्देशहरू अरूले शेयर गरेको वा त्यसबारे कुरा गरिरहेको थाहा पाउनु ।

टाढा बस्न थाल्नु :

अनलाइनमा भएको कुनै घटनाका कारण एपहरू हटाउनु, केही अनलाइन समूहबाट टाढा रहनु, वा साथीहरूसँग कम बोलचाल गर्न थाल्नु ।

यस्ता संकेतहरू चाँडै थाहा पाउनुले तपाईलाई सुरक्षित रहन मद्दत गर्छ । यदि तपाईले यी संकेतहरू आफूमा वा साथीमा देख्नुभयो भने, तपाई एक्लो हुनुहुन्न, सहयोग पाउन सकिन्छ ।



सचेत प्रयोगकर्ता गीता
(Mindful User Gita)

जब म कुनै नकारात्मक कुरा देख्छु, मेरो पहिलो भावना रिस नै हुन्छ। तर म तुरुन्त प्रतिक्रिया जनाउदिन । उत्पीडकहरू मेरो प्रतिक्रिया खोजिरहेका हुन्छन् । उनीहरू मलाई रिसाएको वा डराएको देख्न चाहन्छन्, किनकि त्यसले उनीहरूलाई झन् थप शक्ति दिन्छ। एक सचेत प्रयोगकर्ताको रूपमा, म पहिले आफ्नो सुरक्षा सुनिश्चित गर्छु र प्रमाण सुरक्षित राख्छु। अनलाइन क्रुरताको सामना गर्दा धैर्यता नै तपाईको सबैभन्दा प्रभावकारी हतियार हो।"

डिजिटल सुरक्षा सुनिश्चित गर्ने ६ प्राथमिक कदम

- **सम्पर्क बन्द गर्नुहोस् (Stop Communicating) :** प्रतिक्रिया नदिनुहोस्, जवाफ नदिनुहोस्, वा प्रतिशोध नगर्नुहोस् । तर्क नगर्नुहोस् वा आफूलाई उचित ठहऱ्याउने प्रयास नगर्नुहोस् । सबै अन्तरक्रिया तुरुन्तै समाप्त गर्नुहोस् ।
- **प्रमाण सङ्कलन गर्नुहोस् (Collect Evidence) :** यो सबैभन्दा महत्त्वपूर्ण चरण हो । पोस्टहरू, सन्देशहरू, प्रयोगकर्ता नामहरू र मिति/समयको स्क्रिनसट लिनुहोस् ।

यो प्रमाणलाई इमेल ड्राफ्ट वा क्लाउड फोल्डर जस्ता सुरक्षित, निजी ठाउँमा बचत गर्नुहोस् ।

- **उत्पीडकलाई ब्लक गर्नुहोस् :** प्रयोगकर्तालाई थप सम्पर्क गर्न नसक्ने गरी तुरुन्तै ब्लक गर्न प्लेटफर्मको सेटिङहरू प्रयोग गर्नुहोस् ।
- **प्लेटफर्ममा रिपोर्ट गर्नुहोस्** : हरेक प्रमुख एप (फेसबुक, टिकटक, भाइबर, आदि) मा अन्तर्निर्मित (in-built) "Report Abuse" बटन हुन्छ । यसलाई प्रयोग गर्नुहोस्! प्लेटफर्मले सामग्री हटाउन र प्रयोगकर्तालाई प्रतिबन्ध पनि लगाउन सक्छ ।
- **सहयोग खोज्नुहोस् :** तुरुन्तै विश्वास गर्ने व्यक्तिसँग कुरा गर्नुहोस्: अभिभावक, शिक्षक, दाजु/दिदी वा समुदायका अग्रजसँग सहयोग लिनुहोस्। तपाईंले जम्मा गर्नुभएको प्रमाण उनीहरूलाई देखाउनुहोस्।
- **कानुनी रिपोर्टिङ प्रयोग गर्नुहोस् :** एकपटक तपाईंसँग प्रमाण र समर्थन भएपछि प्रहरीलाई सम्पर्क गर्ने प्रक्रियामा अगाडि बढ्नुहोस् ।

सुरक्षित र सम्मानजनक डिजिटल ठाउँहरू सिर्जना गर्ने

अनलाइन संस्कृतिलाई हरेक प्रयोगकर्ताद्वारा आकार दिइन्छ । त्यसैले दुर्व्यवहार फस्टाउन नसक्ने सकारात्मक वातावरण सिर्जना गर्ने शक्ति तपाईं आफैँसँग छ ।

डिजिटल दयालुपनका सरल नियमहरू

- **समानुभूति अभ्यास गर्नुहोस् :** पोस्ट गर्नुअघि, सोध्नुहोस् , "यदि कसैले मेरो बारेमा यो पोस्ट गऱ्यो भने मलाई कस्तो महसुस हुनेछ ? के यो टिप्पणीले कसैलाई सहयोग गर्छ कि चोट पुऱ्याउँछ?
- **सहमतिलाई प्राथमिकता दिनुहोस्** : अरूको फोटो, भिडियो वा सन्देशहरू उनीहरूको स्पष्ट र सूचित अनुमतिबिना कहिल्यै पोस्ट वा शेयर नगर्नुहोस् । यदि तपाईं निश्चित हुनुहुन्न भने, उत्तर 'होइन' हो भन्ने बुझ्नुहोस्।
- **एक स्मार्ट साक्षी बन्नुहोस् :** यदि तपाईंले दुर्व्यवहार भइरहेको देख्नुभयो भने, यसमा सामेल नहुनुहोस् वा उत्पीडकलाई खुशी नबनाउनुहोस् । बरु, निजी रूपमा पीडितलाई समर्थन गर्नुहोस् र हानिकारक सामग्रीलाई प्लेटफर्ममा रिपोर्ट गर्नुहोस् ।

- **आफ्नो सेटिङहरू व्यवस्थापन गर्नुहोस् :** आफ्ना सबै एपहरूमा गोपनीयता र सुरक्षा सेटिङहरू प्रयोग गर्न सिक्नुहोस् । कसले तपाईंलाई ट्याग गर्न सक्छ, कसले तपाईंलाई सन्देश पठाउन सक्छ र कसले तपाईंको प्रोफाइल हेर्न सक्छ भन्ने कुरा नियन्त्रण गर्नुहोस् ।

शिक्षक विकास
(Teacher Bikash)

"तपाईं जे भन्नुहुन्छ, त्यसका लागि जिम्मेवार हुनुहुन्छ तर तपाईं जे भन्नुहुन्न, त्यसको लागि पनि जिम्मेवार हुनुहुन्छ' भन्ने भनाइ याद गर्नुहोस् । यदि तपाईंले घृणायुक्त बोली वा धम्की देख्नुहुन्छ र चुप लाग्नुहुन्छ भने, तपाईं धम्की दिनेलाई मद्दत गरिरहनुभएको छ । यदि तपाईंले इन्टरनेटमा कसैमाथि दुर्व्यवहार भइरहेको देख्नुभयो भने, आफ्नो क्षमताअनुसार साथ दिनुहोस् र आवश्यक परे आवाज उठाउनुहोस् ।"

डर बिना रिपोर्ट गर्ने !

रिपोर्ट गर्नु भनेको आफ्नै सुरक्षा सुनिश्चित गर्नु र भविष्यमा हुनसक्ने हानी रोक्नु हो। यसले उत्पीडकलाई तपाईं वा अरू कसैलाई पुन: हानी गर्नबाट रोक्न सहयोग गर्छ । नेपाली कानुनी प्रणालीले पनि अनलाइन दुर्व्यवहारका प्रभावितहरूलाई स्पष्ट रूपमा संरक्षण प्रदान गरेको छ।

नेपालमा तपाईंको कानुनी सुरक्षा :

- **इलेक्ट्रोनिक कारोबार ऐन (ETA 2008) :** यो कानुन साइबर बुलिङ, धम्की, मानहानी, र अश्लील सामग्री प्रकाशनमा मुद्दा चलाउन प्रयोग गरिन्छ ।
- **गोपनीयता सम्बन्धी ऐन (२०१८) :** यसले तपाईंको व्यक्तिगत डेटा र फोटोहरू नियन्त्रण गर्ने तपाईंको अधिकारको रक्षा गर्छ । यस ऐनअनुसार, अनुमति बिना पोस्ट वा शेयर गर्नु गैरकानुनी हो।

स्थानीय क्षेत्रका लागि आवश्यक रिपोर्टिङ चरणहरू

१. प्रमाण सङ्कलन गर्नुहोस् र भरपर्दो व्यक्तिको समर्थन खोज्नुहोस् : तपाईंसँग स्क्रिनसटहरू, समय स्ट्याम्पहरू, र उत्पीडकको प्रयोगकर्ता नाम/आईडी छ भन्ने सुनिश्चित गर्नुहोस् ।

२. स्थानीय प्रहरी चौकीमा उजुरी दिनुहोस् : आफ्नो नजिकको प्रहरी चौकी जानुहोस् । तपाईंले काठमाडौं यात्रा गर्नु पर्दैन । आफ्नो डिजिटल प्रमाण आफ्नो स्थानीय प्रहरी चौकीमा लैजानुहोस् । उनीहरूलाई प्रारम्भिक रिपोर्ट फाइल गर्न र साइबर ब्युरोमा फर्वार्ड गर्न तालिम दिइएको हुन्छ ।

३. साइबर ब्युरो (काठमाडौं) लाई सम्पर्क गर्नुहोस् :

- **इमेल :** cyberbureau@nepalpolice.gov.np (यदि तपाईंसँग इमेलमा पहुँच छ भने यो प्रयोग गर्नुहोस्) ।
- **ठेगाना :** नेपाल प्रहरी, साइबर ब्युरो, भोटाहिटी, काठमाडौं (प्रत्यक्ष भेटका लागि) ।
- **ल्याउन नबिर्सनुहोस् :** १) प्रमाण (स्क्रिनसट/प्रिन्टआउट), २) तपाईंको परिचयपत्र र ३) यदि तपाईं १८ वर्ष मुनिको हुनुहुन्छ भने एक भरपर्दो व्यक्तिलाई साथमा ल्याउनुहोस् ।

थप सामग्री : 👉 Cyber Bureau Website

इन्स्पेक्टर सीता
(Inspector Sita)

“हामी अनलाइन ब्ल्याकमेल र मानहानी जस्ता अपराधहरूसँग दैनिक रूपमा सामना गर्छौं। तपाईंले चाल्न सक्ने सबैभन्दा महत्त्वपूर्ण कदम भनेको प्रमाण सुरक्षित राख्नु हो। स्क्रिनसटहरू, समयको रेकर्ड (timestamp) र प्रयोगकर्ताका नामहरू बिना, कानुन लागु गर्न धेरै गाह्रो हुन्छ। साहसी बन्नुहोस्, प्रमाण राख्नुहोस्, र अपराध रिपोर्ट गर्नुहोस्। तपाई सक्रिय रूपमा आफ्नो समुदायलाई सुरक्षित बनाउन र दुर्व्यवहारको चक्र रोक्न मद्दत गर्दै हुनुहुन्छ।”

समीक्षा र ज्ञानको सारांश (Recap)

मुख्य विचार (Key Idea)	विस्तृत सारांश (Detailed Summary)
डिजिटल दुर्व्यवहार (Harassment)	डिजिटल माध्यम प्रयोग गरेर बारम्बार र जानाजानी गरिने हानिकारक व्यवहार
सहमति (Consent)	कसैको निजी डेटा वा सामग्री पोस्ट वा शेयर गर्नुअघि आवश्यक पर्ने स्पष्ट, आवश्यक अनुमति।
व्यक्तिगत बनाम निजी जानकारी	व्यक्तिगत शौक पोस्ट वा शेयर गर्नुहोस्, तर निजी (पासवर्ड, ठेगाना, निजी फोटो) सुरक्षित गर्नुहोस्।
प्रमाण (Evidence)	कानुनी रिपोर्ट फाइल गर्न आवश्यक पर्ने महत्त्वपूर्ण सामग्री प्रमाण (स्क्रिनसट, समय, प्रयोगकर्ता नाम)।
ETA 2008	साइबर अपराधलाई गैरकानुनी र दण्डनीय बनाउने मुख्य नेपाली कानुन।