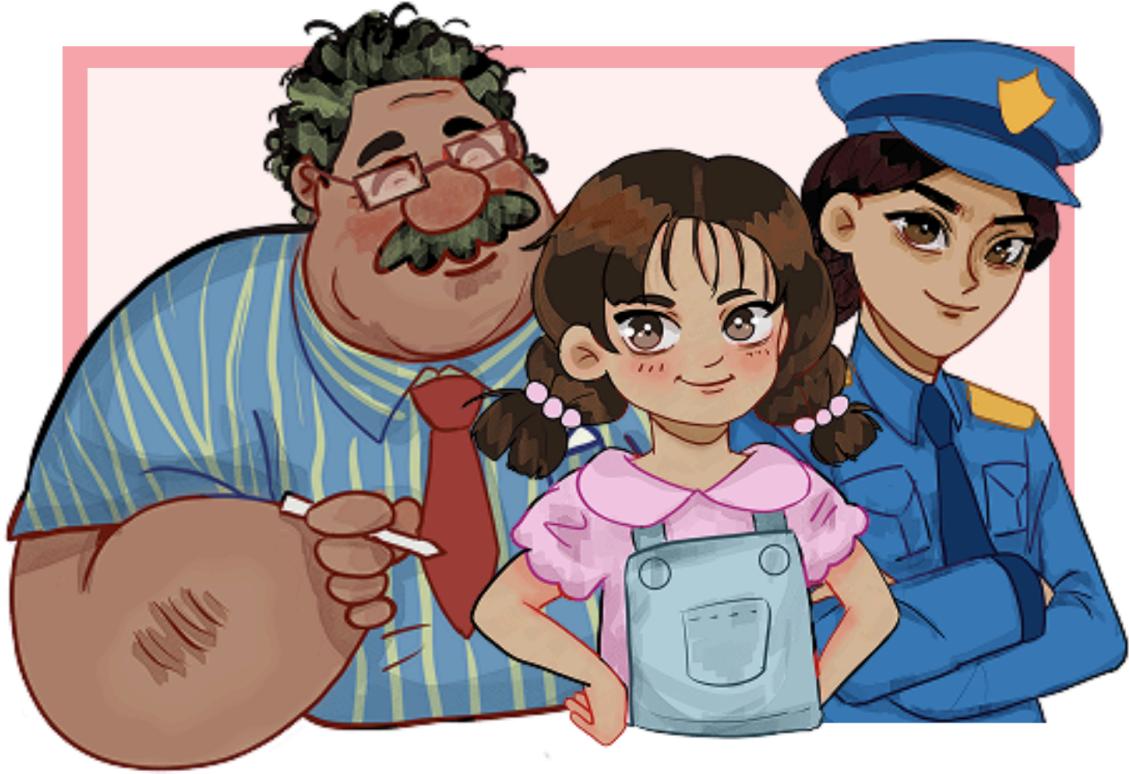


एकाइ २

अधिकार, जिम्मेवारी र अनलाइन व्यवहार





Supported By:

ASML Foundation

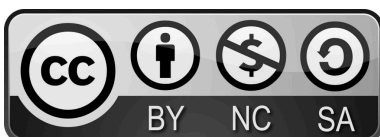


**Alternatives
4 children**

© Karkhana Samuha, 2025

Unless otherwise stated, this work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) license.

<https://creativecommons.org/licenses/by-nc-sa/4.0/>



अधिकार, जिम्मेवारी र अनलाइन व्यवहार

सिकाइका लक्ष्यहरू

यस पाठ एकाइको अन्त्यसम्ममा, विद्यार्थीहरू निम्न कुराहरू गर्न सक्षम हुनेछन् :

- आफ्ना मौलिक **डिजिटल अधिकारहरू (गोपनीयता, पहुँच, अभिव्यक्ति)** र तिनका सम्बन्धित जिम्मेवारीहरू पहिचान गर्न ।
- डेटा र गोपनीयताको सुरक्षालगायत सुरक्षित अनलाइन व्यवहारका लागि व्यावहारिक कदमहरू बुझ्न ।
- **साइबर बुलिङ (Cyberbullying)** र **गलत जानकारी (Misinformation)** जस्ता मुख्य जोखिमहरूलाई चिन्न र सुरक्षित रूपमा प्रतिक्रिया दिन जान्ने हुन ।
- असुरक्षित अनलाइन अनुभवहरूलाई रिपोर्ट गर्न वा समाधान गर्ने तत्कालका कार्यहरू जान्न ।

डिजिटल अधिकार र जिम्मेवारीहरूको सन्तुलन

(The Balance of Digital Rights and Responsibilities)

जसरी देशका नागरिकहरूमा संविधानद्वारा सुरक्षित अधिकारहरू हुन्छन्, त्यसरी नै डिजिटल नागरिकहरूसँग पनि अनलाइनमा अधिकारहरू हुन्छन् । यद्यपि, हरेक अधिकारसँगै समुदायप्रति एउटा **जिम्मेवारी** पनि आउँछ ।

अधिकार र जिम्मेवारीहरू : एक साझेदारी (A Partnership)

तपाईंका डिजिटल अधिकारहरू (Your Digital Rights)	तपाईंका डिजिटल जिम्मेवारीहरू (Your Digital Responsibilities)
<p>गोपनीयताको अधिकार : आफ्नो व्यक्तिगत र निजी जानकारीलाई गलत पहुँचबाट सुरक्षित राख्न पाउने ।</p>	<p>सहमति (Consent) को जिम्मेवारी : अरूको गोपनीयतालाई सम्मान गर्ने र उनीहरूको अनुमतिबिना उनीहरूको डेटा वा फोटोहरू कहिल्यै पोस्ट वा शेयर नगर्ने ।</p>
<p>पहुँचको अधिकार : भेदभावबिना समान रूपमा इन्टरनेट सिक्ने, खोज गर्ने र प्रयोग गर्न पाउने।</p>	<p>प्रयोगको जिम्मेवारी : प्रविधिलाई नैतिक र सकारात्मक उद्देश्यका लागि (जस्तै शिक्षा) प्रयोग गर्ने ।</p>
<p>अभिव्यक्तिको अधिकार : आफ्ना विचार, राय र रचनात्मकतालाई स्वतन्त्र रूपमा पोस्ट वा शेयर गर्न पाउने ।</p>	<p>सम्मानको जिम्मेवारी : घृणात्मक अभिव्यक्ति (Hate speech) वा दुर्व्यवहार (Harassment) नगरिकन सहिष्णुताका साथ आफ्ना विचारहरू व्यक्त गर्ने ।</p>

अनलाइनमा सुरक्षित र सचेत बन्ने (आफ्नो डेटा जोगाउने)

तपाईंले कुनै अपरिचित व्यक्तिलाई आफ्नो घरको ठेगाना वा विद्यालयको परिचयपत्र पक्कै दिनुहुन्न होला, त्यही सावधानी तपाईंको बहुमूल्य डिजिटल जानकारीमा पनि लागु हुन्छ । आफ्नो डेटाको सुरक्षा गर्नु प्राथमिक जिम्मेवारी हो । यसका लागि ध्यान दिनुपर्ने विभिन्न बुँदाहरू यहाँ प्रस्तुत गरिएको छ :

अनिवार्य सुरक्षा चेकलिस्ट :

- **बलियो पासवर्ड :** अनुमान लगाउन गाह्रो हुने जटिल पासवर्डहरू (अक्षर, संख्या र

प्रतीकहरू (symbol) मिलाएर बनाउनुहोस् र बारम्बार परिवर्तन गर्नुहोस् ।

- **दुई-कारक प्रमाणीकरण (2FA) :** (2 Factor Authentication) उपलब्ध हुँदा सधैं सुरक्षाको यो थप तह (Extra layer) प्रयोग गर्नुहोस्, जस्तै: login गर्न password सँगै mobile verification पनि राख्ने ।
- **पोस्ट वा शेयर गर्न सीमित गर्नुहोस् :** निजी फोटोहरू, वित्तीय विवरणहरू (banking details) वा आफ्नो वास्तविक ठेगाना सार्वजनिक रूपमा पोस्ट वा शेयर नगर्नुहोस् ।
- **लिङ्कहरूप्रति शङ्का राख्नुहोस् :** अपरिचित नम्बरहरू वा इमेलहरूबाट आएका लिङ्कहरू भएका सन्देशहरूलाई अत्यधिक सावधानीका साथ प्रयोग गर्नुहोस्; तिनीहरू नक्कली वा हानिकारक (फिसिङ - Phishing) हुन सक्छन् । यदि शंकास्पद लागेमा त्यो लिङ्कको प्रयोग नगर्नुहोस् ।
- **गोपनीयता सेटिङहरू :** तपाईंका सबै एपहरू (Facebook, TikTok आदि) मा गोपनीयता सेटिङहरू (Privacy Settings) नियमित रूपमा जाँच गर्नुहोस् र मिलाउनुहोस्, जसले गर्दा कसले तपाईंका पोस्टहरू हेर्न सक्छ र कसले तपाईंलाई सन्देश पठाउन सक्छ भन्ने नियन्त्रण होस् ।

बलियो पासवर्ड र २ चरण प्रमाणीकरणबारे थप सामग्री : [👉 बलियो पासवर्ड र दुई-](#)

[कारक प्रमाणीकरण \(2FA\)](#)

फिसिङ - Phishing बारे थप सामग्री : [👉 फिसिङ भनेको क हो?](#)



इन्स्पेक्टर सीता
(Inspector Sita)

“डिजिटल नागरिकका रूपमा आफ्नो डेटा सुरक्षित राख्नु भनेको अनलाइन संसारमा आफ्नो पहिचान र गोपनीयताको रक्षा गर्नु हो। अचेल फिसिङ (Phishing) जस्ता छलकपटपूर्ण सन्देश र शंकास्पद लिङ्कहरू मार्फत तपाईंको निजी जानकारी चोर्ने जोखिम निकै बढेको छ। यसरी अनुमति बिना कसैको डेटामा अनधिकृत पहुँच पुऱ्याउनु विद्युतीय कारोबार ऐन (ETA 2008) अनुसार गम्भीर कानुनी अपराध मानिन्छ। त्यसैले, कमजोर पासवर्ड राख्ने वा नबुझी जुनसुकै लिङ्कमा क्लिक गर्ने स-साना लापरवाहीले तपाईंलाई साइबर अपराधीको सिकार बनाउन सक्छ।”

प्रमुख अनलाइन जोखिमहरू

क. साइबर बुलिङ र दुर्व्यवहार (Cyberbullying and Harassment)

साइबर बुलिङ भन्नाले इन्टरनेटको प्रयोगद्वारा कसैलाई बारम्बार चोट पुर्याउने, धम्की दिने वा अपमान गर्ने कार्य हो । यसले मनोवैज्ञानिक क्षति पुर्याउँछ ।

यदि तपाईं साइबर बुलिङको सिकार वा साक्षी हुनुहुन्छ भने :

- **प्रतिक्रिया नदिनुहोस् (Don't Respond)** : कहिल्यै बदलाको भावले प्रतिक्रिया वा तर्क नगर्नुहोस् । यसले उनीहरूले गलत क्रियाकलाप दोहोर्‍याउने सम्भावना बढाउँछ र तपाईंको डिजिटल सुरक्षामा थप हानी हुने जोखिम बढाउँछ ।
- **प्रमाण सङ्कलन गर्नुहोस्** : हानिकारक टिप्पणी वा सन्देशहरू र ती पोस्ट गर्ने/पठाउने व्यक्तिको प्रयोगकर्ता नाम तथा प्रोफाइल देखिनेगरी तुरुन्त स्क्रिनसट लिनुहोस् ।
- **सहयोग खोज्नुहोस्** : एक विश्वसनीय व्यक्ति (Trusted adult), अभिभावक, शिक्षक, विद्यालयका परामर्शदाता, ठूलो दाजु/दिदी लाई भन्नुहोस् ।
- **रिपोर्ट गर्नुहोस् र Block गर्नुहोस् (Report & Block)** : प्लेटफर्ममा भएको "Report Abuse" सुविधा को प्रयोग गर्नुहोस् र अपराधीलाई तुरुन्तै "Block" गरेर रोक्नुहोस् ।

थप सामग्री : [👉 Cyberbullying](#)

ख. गलत जानकारी र झुटा समाचार (Misinformation and Fake News)

गलत जानकारी (Misinformation) भनेको अनलाइनमा जान वा अन्जान रूपमा पोस्ट वा शेयर गरिएको झुटो जानकारी हो । यो प्रायः छिट्टै फैलन्छ र त्रास वा विभाजन पैदा गर्न सक्छ ।

पोस्ट वा शेयर गर्नुअघि :

- **स्रोत जाँच गर्नुहोस्** : के यो भरपर्दो, प्रमाणित समाचार एजेन्सीबाट आएको हो ? वा कुनै अनियमित पृष्ठबाट ?
- **प्रमाणित गर्नुहोस् (Verify)** : के त्यो कथा कम्तीमा **दुईवटा फरक, विश्वसनीय** समाचार वेबसाइटहरूमा देखिएको छ ?

- **उद्देश्य पहिचान गर्नुहोस्** : सोध्नुहोस् - "यो किन पोस्ट गरियो ? के यो मलाई उक्साउन, तर्साउन वा पैसाको लागि क्लिक गर्न लगाउनको लागि हो कि ?" यदि उद्देश्य हेरफेर गर्ने (Manipulative) जस्तो लाग्छ भने, यसलाई पोस्ट वा शेयर नगर्नुहोस् ।
- **शङ्का लागेमा रोक्नुहोस्** : यदि तपाईं अनिश्चित हुनुहुन्छ भने, यसलाई पोस्ट वा शेयर नगर्नुहोस् । **अफवाह रोक्ने जिम्मेवारी** तपाईंसँग छ ।

थप सामग्री : 📌 **गलत जानकारी र झुटा समाचार**

क्रियाकलाप : मेरो अनलाइन आचारसंहिता (My Online Code of Conduct)

आफ्नो व्यक्तिगत **डिजिटल जिम्मेवारी शपथ (Digital Responsibility Pledge)** सिर्जना गर्नुहोस् । जिम्मेवार कार्यका लागि तीनवटा वाचा र तपाईंले तुरुन्तै गर्न रोक्ने कार्यका लागि तीनवटा वाचा लेख्नुहोस् ।

मेरो डिजिटल जिम्मेवारी शपथ

<p>✅ मैले गर्ने वाचा (Commitments)</p>	<p>❌ मैले गर्न रोक्ने वाचा (Actions to Stop)</p>
<p>१. म सधैं मेरा पासवर्डहरू सुरक्षित राख्नेछु र 2FA प्रयोग गर्नेछु ।</p>	<p>१. म कहिल्यै पनि पुष्टी नभएको (Unverified) वा झुटो समाचार पोस्ट वा शेयर गर्दिन ।</p>
<p>२. म फरक मत हुँदा पनि मेरो विचारलाई आदरपूर्वक व्यक्त गर्नेछु ।</p>	<p>२. म कुनै पनि अनलाइन छलफलमा कसैलाई पनि गाली वा दुर्व्यवहार गर्दिन ।</p>
<p>३. म साइबर बुलिङको कुनै पनि घटनामा बोल्ने वा रिपोर्ट गर्नेछु ।</p>	<p>३. म अरूको निजी जानकारी वा फोटो उनीहरूको अनुमतिबिना पोस्ट गर्दिन ।</p>

पाठ एकाइको मुख्य सारांश

अवधारणा (Concept)	पाठ (Lesson)
डिजिटल अधिकारहरू	गोपनीयता, पहुँच र अभिव्यक्तिको अधिकार ।
डिजिटल जिम्मेवारी	गोपनीयताको सम्मान गर्ने, बुद्धिमानीपूर्वक प्रविधि प्रयोग गर्ने र आदरपूर्वक बोल्ने ।
साइबर बुलिङ	बारम्बार गरिने अनलाइन हानी प्रतिक्रिया: सधैं स्क्रिनसट लिनुहोस्, जिम्मेवार व्यक्तिलाई भन्नुहोस्, रिपोर्ट गर्नुहोस् ।
गलत जानकारी	झुटो सामग्री प्रतिक्रिया: सधैं स्रोत प्रमाणित गर्नुहोस्, उद्देश्यमा प्रश्न गर्नुहोस्, पोस्ट वा शेयर गर्न रोक्नुहोस् ।