जिल्ला नेटवर्कको स्वीकार्य प्रयोग

उद्देश्य

यस नीतिले सबै रोचेस्टर सिटी स्कूल डिस्ट्रिक्ट ("जिल्ला") बोर्ड सदस्यहरू, कर्मचारीहरू, विद्यार्थीहरू, परामर्शदाताहरू, साझेदारहरू, र अतिथिहरूद्वारा जिल्लाको नेटवर्कको प्रयोगलाई नियन्त्रण गर्ने मापदण्ड र अपेक्षाहरू सेट गर्दछ। यो नीति जिल्ला सञ्जालको नैतिक, कानुनी, र विद्यालय-सम्बन्धित प्रयोगलाई बढावा दिनको लागि हो। सबै इलेक्ट्रोनिक उपकरणहरू यस नीति अन्तर्गत नियन्त्रित हुनेछ जब त्यस्ता उपकरणहरू जिल्ला नेटवर्कमा संलग्न हुन्छन्।

जिम्मेवारी

जिल्लाले उपलब्ध गराएको कम्प्यूटर, वायर्ड र अनवायर नेटवर्कहरू, इमेल र इन्टरनेट पहुँचको उद्देश्य वैध जिल्ला कार्य, अनुसन्धान र शिक्षाको समर्थनमा सञ्चारलाई सहज बनाउनु हो। प्रयोगकर्ताको रूपमा योग्य रहनको लागि, यस्तो प्रयोगले जिल्लाको शैक्षिक उद्देश्य र कार्य जिम्मेवारीहरूलाई समर्थन गर्नुपर्छ। पहुँच एक विशेषाधिकार हो, अधिकार होइन र पहुँच जिम्मेवारी समावेश गर्दछ।

परिभाषाहरू

१. जिल्ला सञ्जाल: सबै जिल्लाको स्वामित्व वा इजाजतपत्र प्राप्त कम्प्युटरहरू, वायर्ड र अनवायर नेटवर्कहरू, इमेल र टेलिफोन, हार्डवेयर, सफ्टवेयर, र सम्बन्धित प्रविधिहरू, सबै नेटवर्कहरू, तारहरू, र सञ्चार उपकरणहरू सहित।

२. इलेक्ट्रोनिक जानकारी: जिल्ला नेटवर्कमा भण्डारण गरिएका सबै इ-मेल, अडियो फाइलहरू र इलेक्ट्रोनिक डाटा, फाइलहरू वा अन्य रेकर्डहरू

३. शैक्षिक उद्देश्यहरू: ती कार्यहरू प्रत्यक्ष रूपमा जिल्लाको शैक्षिक, निर्देशनात्मक, प्रशासनिक, व्यवसाय, र समर्थन सेवा मिसनहरूलाई प्रवर्द्धन गर्ने र कुनै पनि जिल्ला निर्देशन, परियोजना, काम, कार्य असाइनमेन्ट, कार्य, वा कार्य जसको लागि प्रयोगकर्ता जिम्मेवार छ।

४. अनुपयुक्त सामग्रीहरू: वस्तुहरूको पाठ, ग्राफिक, चित्रात्मक, वा श्रवण प्रतिनिधित्वहरू जुन, समग्र रूपमा लीएको र विद्यार्थीहरूको हितको सन्दर्भमा, नग्नता, यौन, वा उत्सर्जनमा पूर्व रुचिको लागि अपील गर्दछ; विद्यार्थीहरूको लागि गम्भीर साहित्यिक, कलात्मक, राजनीतिक, वा वैज्ञानिक मूल्यको कमी नहुने सामग्रीहरू; जाति, धर्म, लिङ्ग, राष्ट्रियता, यौन झुकावको आधारमा अरू विरुद्ध भेदभाव वा उत्पीडनलाई बढावा दिने सामग्रीहरू; व्यक्तिलाई गैरकानूनी गतिविधिहरूमा संलग्न हुन सक्षम पार्ने सीपहरू सिकाउने उद्देश्यका सामग्रीहरू; वा कानूनको उल्लङ्घन गर्ने वा शिक्षा बोर्ड, सुपरिटेन्डेन्ट विनियम वा जिल्लाको शैक्षिक मिशनको नीतिहरूसँग असंगत सामग्रीहरू।

५. इन्टरनेट पहुँच: इन्टरनेट सर्भरहरू र प्रयोगकर्ताहरूसँग जडान गर्न प्रयोग गरिएका सबै विधिहरू, र इ-मेल सहित कोष वा सुविधा स्रोतहरूको पर्वाह नगरी पहुँच प्रदान गर्ने सबै विधिहरू।

६. प्रतिबन्धित जानकारी: कुनै पनि डेटा वा जानकारी जसको लागि पहुँच गर्ने व्यक्तिको शैक्षिक उद्देश्य छैन। यो सार्वजनिक मान्न सकिने जानकारीसँग पनि सम्बन्धित छ जहाँ त्यस्ता जानकारीले जिल्ला र कर्मचारीहरूको लागि लाभदायक तरिकाले प्रयोगकर्ता जिम्मेवारीहरूलाई समर्थन गर्दैन।

७. टेक्नोलोजी सुरक्षा उपाय: एक इन्टरनेट फिल्टरिङ टेक्नोलोजी जुन पहिचान गरिएका मापदण्डहरूमा आधारित इन्टरनेटको चयन गरिएका भागहरूमा पहुँच सीमित गर्न डिजाइन गरिएको हो। जिल्लामा यसको अभिप्रेत प्रयोग अनुपयुक्त सामग्रीमा पहुँच सीमित गर्नु हो। अनाधिकृत उपकरण: कुनै पनि यन्त्र जुन सुपरिटेन्डेन्ट वा डिस्ट्रिक्ट कम्प्युटर वा डिस्ट्रिक्ट नेटवर्कमा जडान हुनको लागि अनुमोदित छैन, वायरलेस पहुँच पोइन्टहरू, नेटवर्क राउटरहरू र नेटवर्क स्विचहरू जस्ता व्यक्तिगत नेटवर्क उपकरणहरूमा मात्र सीमित छैन।

८. प्रयोगकर्ता: कुनै पनि शिक्षा बोर्ड सदस्य, जिल्ला कर्मचारी, विद्यार्थी, परामर्शदाता, साझेदार, अतिथि वा जिल्ला नेटवर्क प्रयोग गर्न अधिकृत व्यक्ति।

प्रक्रिया

१. इलेक्ट्रोनिक डाटा र सूचना सुरक्षा को व्यवस्थापन

प्रयोगकर्ताहरूले जानकारी र।वा कम्प्युटर प्रणालीहरू मात्र पहुँच गर्न सक्छन जसमा उनीहरूलाई अधिकार छ र उनीहरूलाई उनीहरूको असाइनमेन्ट र जिम्मेवारीहरूको लागि आवश्यक छ।

क. प्रयोगकर्ताहरू आफ्नै व्यक्तिगत खाताहरूको लागि जिम्मेवार छन्।

१. प्रयोगकर्ताहरूले सूचना व्यवस्थापन र प्रविधि विभाग ("आइएमएनटि") द्वारा निर्देशित पासवर्डहरू परिवर्तन गरेर र तिनीहरूको पासवर्डहरू कडा रूपमा गोप्य राखेर आफ्नो खाताको सुरक्षा सुरक्षित गर्न आवश्यक छ।

२. प्रयोगकर्ताहरूलाई खाता र पासवर्डहरू साझेदारी गर्न स्पष्ट रूपमा निषेध गरिएको छ।

३. उल्लङ्घनहरू जुन व्यक्तिगत खाता नाममा पत्ता लगाउन सकिन्छ खाता मालिकको जिम्मेवारीको रूपमा व्यवहार गर्न सकिन्छ।

ख.आइएमएनटि ले प्रोटोकलहरू विकास र कार्यान्वयन गर्नेछ ताकि प्रयोगकर्ताहरू पूर्वनिर्धारित अवधिको लागि तिनीहरूको कम्प्युटरबाट टाढा हुँदा कम्प्युटरहरू स्वचालित रूपमा लक हुन सक्छन्। प्रयोगकर्ताहरूले अरूलाई आफ्नो कम्प्युटर प्रयोग गर्न अनुमति दिनु अघि लग अफ गर्न आवश्यक छ।

यो नियमन बमोजिम सबै लागू हुने सुरक्षा प्रक्रियाहरू बारे सचेत हुनु र पालना गर्नु प्रत्येक प्रयोगकर्ताको जिम्मेवारी हो।

ग. प्रयोगकर्ताहरूले आफ्नो इलेक्ट्रोनिक डाटा सुरक्षित गर्नुपर्छ। संवेदनशील फाइलहरू सुरक्षित स्थानमा सुरक्षित गरिनु पर्छ जस्तै एक व्यक्तिको नेटवर्क फोल्डर।डाइरेक्टरी वा हटाउन सकिने डिस्क जुन त्यसपछि लक गरिएको फाइल क्याबिनेटमा सुरक्षित हुन्छ, वा सुरक्षित जिल्ला क्लाउड स्थान (जस्तै गुगल क्लाउड, वन ड्राइभ)।

घ. प्रयोगकर्ताहरूले आफ्नो कम्प्युटरमा भण्डारण गरिएका महत्वपूर्ण फाइलहरूको जगेडा प्रतिलिपिहरू बनाउनु पर्छ र प्रतिलिपिहरू सुरक्षित ठाउँमा भण्डार गरिएको छ भनी सुनिश्चित गर्नुपर्छ।

ङ. जिल्ला डाटा र सूचना - कर्मचारीहरूले मात्र जानकारी पहुँच गर्नेछन जुन; आफ्नो जिल्ला कर्तव्यहरू अभिप्रेत उद्देश्य अनुरूप गर्न आवश्यक छ; आचार संहिता संग संगत छ; र **प्रतिबन्धित जानकारीको** रूपमा योग्य छैन।

२. भौतिक सुरक्षा

कम्प्युटर प्रणाली उपकरणहरू सुरक्षित भौतिक वातावरणमा अवस्थित र मर्मत गरिएको हुनुपर्छ। प्रयोगकर्ताहरू कम्प्युटर र सम्बन्धित प्रविधिको लागि निम्न भौतिक सुरक्षा प्रावधानहरूसँग सहयोग गर्न जिम्मेवार छन्।

क. जब कर्मचारी सदस्यहरू क्षेत्रको पर्यवेक्षण गर्न उपस्थित हुँदैनन्, सबै क्षेत्रहरू (स्थायी वा अस्थायी भण्डारण सहित) आवास मूल्यवान कम्प्युटर उपकरणहरू सुरक्षित हुनुपर्छ।

ख. स्थानान्तरण वा हटाउन पाइने छैन। कुनै पनि कम्प्युटर वा सम्बन्धित उपकरणहरू त्यस भवनमा तोकिएको जिल्ला कम्प्युटर प्राविधिकको निरीक्षणमा मात्र एक स्थानबाट अर्को स्थानमा सार्न सकिन्छ।

ग. ल्यापटप कम्प्युटर जारी गरेको प्रयोगकर्ताहरूले कम्प्युटर कब्जा गर्दा हात रसिदमा हस्ताक्षर गर्नुपर्छ। प्रयोगकर्ताले जिल्ला छोड्नु वा अर्को विद्यालय वा कार्यालयमा स्थानान्तरण गर्नु अघि ल्यापटप आइएमएनटि कम्प्युटर सेवा सम्पर्क (केन्द्रीय कार्यालयमा अवस्थित) वा स्कूल प्राविधिकलाई फिर्ता गरिनुपर्छ।

घ. हेल्प डेस्कले सबै कम्प्युटरहरू, कम्प्युटर उपकरणहरू र सेलुलर टेलिफोनहरूको डाटाबेस एक हात रसिद अन्तर्गत साइन आउट गर्नेछ। उपकरण कब्जा गर्ने व्यक्तिको जिम्मेवारी हो र हातको रसिदमा हस्ताक्षर गर्ने मद्दत डेस्कलाई सूचित गर्ने कि उनीहरूले उपकरणहरू फिर्ता गरेका छन ताकि उनीहरूको नाम उपकरणको स्वामित्वमा रहेको प्रयोगकर्ताको रूपमा डाटाबेसबाट हटाउन सकिन्छ।

ङ. जिल्ला कर्मचारीहरूले हराएको र।वा चोरी भएको उपकरण निम्नद्वारा रिपोर्ट गर्नुपर्छ:

i. प्रहरीलाई खबर गर्ने र चोरीको उपकरणको प्रहरी रिपोर्ट दर्ता गर्ने।

१) प्रहरी प्रतिवेदनको प्रतिलिपि प्राप्त गरी एउटा प्रतिलिपि निम्नलाई पठाउनुहोस्:

क) सुरक्षा र सुरक्षा कार्यालय को निर्देशक; र

ख) आइएमएनटि को सूचना प्रविधि अधिकारी।

२) हराएको, चोरी भएको वा क्षतिग्रस्त कम्प्युटर उपकरण रिपोर्ट फारम पूरा गर्दै सबै हराएका वस्तुहरूलाई तिनीहरूको क्रम संख्या, मेक, मोडेल नम्बर र अनुमानित लागतहरू सूचीबद्ध गर्दै। प्रतिलिपिहरू त्यसपछि सुरक्षा र सुरक्षाको कार्यालयका निर्देशक र आइएमएनटि को सूचना प्रविधि अधिकारीलाई दीनुपर्छ।

३. प्रणाली र अनुप्रयोग सुरक्षा

क. प्रयोगकर्ताहरूले हेल्प डेस्कको अनुमति बिना कुनै पनि उद्देश्यका लागि कुनै पनि कम्प्युटरमा स्थापना गरिएका सुरक्षा सेटिङहरू वा उपायहरू (जस्तै एन्टिभाइरस सफ्टवेयर) स्थापना गर्न वा असक्षम वा परिमार्जन गर्ने छैनन्।

ख. प्रयोगकर्ताहरूले हेल्प डेस्कको अनुमति बिना प्रणाली सेटिङहरू परिवर्तन गर्नु हुँदैन।

ग. जिल्ला सफ्टवेयर र अनुप्रयोगहरू गैर-जिल्ला कम्प्युटरमा स्थापना वा प्रतिलिपि गर्न सकिँदैन, सूचना प्रविधि अधिकारीले लिखित रूपमा अधिकार दिएको बाहेक।

४. नेटवर्क सुरक्षा

जिल्ला बाहिरका नेटवर्कहरूमा पाइने जानकारीको लागि जिल्ला जिम्मेवार हुँदैन, उदाहरणका लागि, इन्टरनेट सहित। जिल्लाको माध्यमबाट पहुँच हुने अन्य प्रणाली वा इन्टरनेट साइटहरूमा रहेको जानकारीमाथि जिल्लाको नियन्त्रण छैन। जिल्ला बाहिरका केही साइटहरू र प्रणालीहरूमा अपमानजनक, गलत, अपमानजनक, अश्लील, अपवित्र, यौन उन्मुख, धम्की दिने, जातीय रूपमा आपत्तिजनक, वा अवैध सामग्री हुन सक्छ।

क. नेटवर्कमा सामग्रीको पहुँच वा आयात शैक्षिक उद्देश्यका लागि हो भनी सुनिश्चित गर्न प्रयोगकर्ताहरू जिम्मेवार छन्।

ख.जिल्ला प्रणाली वा इन्टरनेट साइटबाट उद्देश्यपूर्वक पोस्ट गरिएको वा लिङ्क गरिएको कुनै पनि सामग्री वा जानकारी यस नियममा परिभाषित गरिए अनुसार जिल्लाको शैक्षिक वा व्यावसायिक उद्देश्यसँग मेल खानुपर्छ।

ग. प्रयोगकर्ताहरू सबै संघीय र राज्य कानूनहरू, बोर्ड नीतिहरू र उनीहरूले प्रयोग गर्ने कम्प्युटर प्रणाली (हरू) मा लागू सुपरिटेन्डेन्ट नियमहरू पालना गर्न जिम्मेवार छन्, जसमा जिल्ला उपकरणहरूबाट इन्टरनेट मार्फत पहुँच गरिन्छ।

घ. उपअनुच्छेद ई मा प्रदान गरिएको बाहेक। र फ़। तल, जिल्ला कर्मचारीहरू, साझेदारहरू, वा परामर्शदाताहरूद्वारा व्यक्तिगत रूपमा स्वामित्वमा रहेका उपकरणहरू जिल्ला सञ्जालमा वा सिधै कुनै पनि जिल्लाको स्वामित्वमा रहेका उपकरणहरूमा जडान हुन सक्दैन।

ङ. आफ्नो कर्पोरेट ल्यापटप वा डेस्कटप कम्प्युटरहरू जिल्लाको नेटवर्कमा जडान गर्न ठेकेदार वा परामर्शदाताहरूको अनुरोधहरूलाई सूचना प्रविधि अधिकारी वा नियुक्त व्यक्तिले केस-दर-केसको आधारमा लिखित रूपमा विचार गरी अनुमोदन गर्नुपर्छ।

च. स्वीकृत ठेकेदारहरूले नेटवर्क पहुँच अनुरोध फारममा हस्ताक्षर गर्नुपर्छ।

छ. सबै प्रयोगकर्ताहरूका लागि अनुमोदित रिमोट पहुँच वा भर्चुअल निजी नेटवर्क ("भिपिएन") मात्र इन्टरनेट मार्फत जिल्ला वेब पृष्ठहरू र जिल्ला इ-मेल प्रणालीमा छ। सूचना प्रविधि अधिकारीको स्पष्ट लिखित अधिकार बाहेक अन्य सबै जिल्ला कम्प्युटर प्रणालीहरूमा रिमोट पहुँच अनुमति छैन।

i. भिपिएन पहुँच जिल्लाको स्वामित्वमा रहेको विन्डोमा आधारित कम्प्युटर प्रणाली उपकरणहरू प्रयोग गर्ने जिल्ला कर्मचारीहरूलाई मात्र दीन्छ।

ii. कर्मचारीहरूले महत्त्वपूर्ण व्यापार औचित्यका साथ ठेकेदारहरूका लागि भिपिएन पहुँच अनुरोध गर्न सक्छन र सूचना प्रविधि अधिकारी वा नियुक्त व्यक्तिद्वारा केस-द्वारा-केस आधारमा अनुमोदन हुन सक्छ। स्वीकृत ठेकेदारहरूले जिल्लाको भिपिएन पहुँच अनुरोध फारममा हस्ताक्षर गर्नुपर्छ।

५. आचरण र प्रयोग गर्नुहोस्

क. सबै कम्प्युटर सुविधाहरू, जिल्ला नेटवर्क, र अन्य प्रविधि स्रोतहरू शैक्षिक उद्देश्यका लागि प्रयोग गरिन्छ र जिल्ला समीक्षाको अधीनमा छन र लग इन र अभिलेख गर्न सकिन्छ।

ख. जिल्ला इ-मेल जिल्ला शैक्षिक उद्देश्यका लागि मात्र हो। सबै इमेलहरू जिल्ला समीक्षाको अधीनमा छन र लग इन र अभिलेख गरिनेछ।

i. आइएमएनटि ले सबै कर्मचारीहरूलाई आधिकारिक जिल्ला इ-मेल ठेगाना प्रदान गर्नेछ। यो आधिकारिक ठेगानामा जिल्लाले कर्मचारीहरूलाई इमेल संचार पठाउनेछ। यो आधिकारिक इ-मेल ठेगाना जिल्लाको एक्सचेन्ज इ-मेल प्रणालीको लागि ग्लोबल ठेगाना पुस्तिकामा सूचीबद्ध हुनेछ।

ii. इ-मेल प्रणालीमा सञ्चार व्यावसायिक र कार्यस्थलको लागि उपयुक्त हुनुपर्छ।

iii. मेल वा मेल मार्गहरूको उत्पत्तिलाई अस्पष्ट गर्नका लागि मेल हेडर वा राउटिङ जानकारीलाई झूटो बनाउन निषेध गरिएको छ।

iv. अर्कोलाई एट्रिब्यूट गरिएको सन्देशको सामग्री परिवर्तन गर्न अनुमति छैन जबसम्म परिवर्तनहरू सञ्चारमा स्पष्ट रूपमा भनिएको छैन।

v. जिल्लाले अर्को इ-मेल ठेगाना (जस्तै @हटमेल.कम, @यहु.कम, @जिमेल.कम, आदि) मा इलेक्ट्रोनिक रूपमा इ-मेल रिडिरेक्ट गर्न समर्थन गर्दैन।

ग. संचारहरू समय-महत्वपूर्ण हुन सक्छ भन्ने कुरालाई ध्यानमा राख्दै, प्रयोगकर्ताहरूले जिल्ला सञ्चारको साथ अद्यावधिक रहन बारम्बार र लगातार आधारमा आफ्नो आधिकारिक इ-मेल ठेगाना जाँच गर्ने अपेक्षा गरिन्छ।

घ. सबै प्रयोगकर्ताहरूलाई कुनै पनि गैरकानूनी गतिविधि वा अन्य कुनै पनि गतिविधिहरूमा संलग्न हुनबाट निषेध गरिएको छ जसले कुनै पनि हिसाबले जिल्लालाई बदनाम गराउनेछ।

ङ. यद्यपि कम्प्युटर सुविधाहरूको प्रत्येक अनुपयुक्त आचरण र प्रयोगलाई पहिचान गर्न असम्भव छ, कम्प्युटर र सञ्जाल प्रयोग उल्लंघनका निम्न उदाहरणहरू स्पष्ट रूपमा निषेधित छन्:

i. जिल्ला सञ्जालको कुनै पनि भागसँग छेडछाड गर्ने वा अरूलाई छेडछाड गर्न मद्दत गर्ने (जस्तै अपरेटिङ सिस्टम, व्यक्तिगत खाताहरू, नेटवर्क-साझेदारी फोल्डर, सफ्टवेयर, नेटवर्किङ सुविधाहरू, र/वा अन्य कार्यक्रमहरू) र/वा उपकरण क्षतिको कुनै पनि अनधिकृत परिवर्तन।

ii. पासवर्डहरू डिक्रिप्ट गर्ने, हार्डवेयर उपकरणहरू वा सफ्टवेयर अनुप्रयोगहरू प्रयोग गरेर पासवर्डहरूको अनाधिकृत कब्जा, र/वा अनाधिकृत उच्च-स्तर पहुँच वा विशेषाधिकारहरू प्राप्त गर्ने वा त्यसो गर्ने प्रयास गर्ने।

iii. अन्य प्रयोगकर्ताहरूको नेटवर्क पहुँच वा कम्प्युटर प्रयोगमा जानाजानी हस्तक्षेप गर्दै।

iv. भाषा, तस्विर वा अन्य सामग्रीको प्रयोग, स्वामित्व वा वितरण गर्ने वा अपमानजनक, निन्दा गर्ने वा अरूलाई सताउने कार्यहरू लिने।

v. अनुपयुक्त सामग्रीहरू प्रयोग गर्ने, राख्ने वा वितरण गर्ने।

vi. जिल्ला कम्प्युटर प्रणालीको अभिप्रेत कार्यलाई हानि पुऱ्याउन वा बिगार्न सक्ने भाइरस वा वर्महरू जस्ता कोडहरू प्रस्तुत गर्दै।

vii. सुपरिटेन्डेन्ट वा नियुक्तिको अख्तियारी बिना कुनै पनि जिल्ला कम्प्युटर वा जिल्ला नेटवर्कमा अनाधिकृत उपकरणहरू संलग्न गर्ने।

viii. सर्कमभेन्टिङ टेक्नोलोजी सुरक्षा उपायहरू, जसलाई नेटवर्क सुरक्षा वा फिल्टरिङ प्रविधि पनि भनिन्छ।

ix.अन्य प्रयोगकर्ताहरूको इमेल पढ्ने, मेटाउने, प्रतिलिपि गर्ने, फोर्ज गर्ने, वा परिमार्जन गर्ने वा त्यसो गर्ने प्रयास गर्ने।

x. सुपरिटेन्डेन्ट वा नियुक्त व्यक्तिको स्पष्ट लिखित अधिकार बिना अन्य प्रयोगकर्ताहरूको डाटा फाइलहरू पढ्ने, मेटाउने, प्रतिलिपि गर्ने, फर्वार्ड गर्ने, प्रिन्ट गर्ने, साझेदारी गर्ने, वा परिमार्जन गर्ने।

xi .अर्कोलाई आफ्नो व्यक्तिगत जिल्ला इ-मेल ठेगाना, खाता, वा पासवर्ड प्रयोग गर्न अनुमति दिँदै।

xii. अर्को व्यक्तिको व्यक्तिगत जिल्ला नेटवर्क खाता, नेटवर्क फोल्डरहरू, वा पासवर्ड प्रयोग गर्न अनुमति दिँदै।

xiii. जिल्ला प्रणालीहरूमा व्यावसायिक विज्ञापनहरू, व्यक्तिगत अनुरोधहरू, चेन लेटरहरू, वा गैर-शैक्षिक खेलहरू प्रयोग गर्दै।

xiv. अधिकार बिना प्रतिलिपि अधिकार सामग्री र सफ्टवेयर प्रतिलिपि वा स्थानान्तरण।

xv. उचित प्राधिकरण बिना विद्यार्थी वा कर्मचारीहरू बारे व्यक्तिगत रूपमा पहिचान योग्य, गोप्य वा गलत जानकारी पोस्ट गर्न जिल्ला नेटवर्कहरू प्रयोग गर्दै।

xvi. व्यक्तिगत लाभ वा कुनै गैरकानूनी वा अनाधिकृत गतिविधिको लागि जिल्ला नेटवर्क वा कम्प्युटर प्रणाली प्रयोग गर्दै।

xvii. राजनीतिक वा धार्मिक कारणहरूलाई बढावा दिनुहोस्।

xviii. गोप्य जिल्ला वा विद्यार्थी डेटा वा सूचना सुपरिटेन्डेन्ट वा नियुक्त व्यक्तिको अख्तियारी बिना वितरण।

xix. व्यक्तिगत आर्थिक लाभ बढाउनको लागि कुनै पनि गतिविधि।

xx. कुनै अवैध उद्देश्य वा कार्य।

च. सबै प्रयोगकर्ताहरूलाई जानाजानी पहुँच गर्न वा अनुपयुक्त सामग्री पहुँच गर्ने प्रयास गर्न निषेध गरिएको छ। इन्टरनेटको विद्यार्थी र कर्मचारीको प्रयोगलाई प्रविधि र प्रत्यक्ष पर्यवेक्षण सहित तर यतिमै सीमित नभएका विभिन्न विधिहरूद्वारा निगरानी गरिनेछ।

i. आइएमएनटि निर्देशक वा नियुक्त व्यक्तिको विवेकमा, आइएमएनटिले बालबालिकाको इन्टरनेट सुरक्षा ऐनले आवश्यक भएअनुसार इन्टरनेट पहुँचलाई रोक्न वा फिल्टर गर्ने उपायहरू लिनेछ। न्यूनतम रूपमा, साइटहरूको निम्न कोटीहरू अवरुद्ध हुनेछन्:

१) हिंसा - यो वर्गले हिंसात्मक कार्यहरूमा भाग लिनको लागि भिजुअल प्रतिनिधित्व वा निमन्त्रणाहरू समावेश गर्ने साइटहरूलाई जनाउँछ। यसमा युद्ध, अपराध, ठट्टा, हेजिङ, इत्यादि समावेश हुन सक्छ। हिंसात्मक कार्यलाई कुनै

पनि गतिविधि मान्न सकिन्छ जसले अर्को जीवित प्राणीलाई चोट पुर्याउन डिजाइन गरिएको शारीरिक बल प्रयोग गर्दछ।

२) हतियार।बमहरू - यो वर्गले हतियार र।वा बमको प्रयोग र बम बनाउने कुनै पनि साइटलाई जनाउँछ। यसले बन्दुक नियन्त्रण वा वैध सामाजिक मुद्दाहरूसँग सम्बन्धित साइटहरू समावेश गर्दैन।

३) वयस्क विषयवस्तु र सामग्री - यो श्रेणीले साइटहरूलाई बुझाउँछ जुन प्रकृतिमा वयस्क हो र अन्य मूल्याङ्कन कोटीहरूमा परिभाषित गरिएको छैन।

४) पोर्नोग्राफी - यो श्रेणीले हल्का चित्रण, सफ्ट पोर्नोग्राफी र हार्ड-कोर पोर्नोग्राफी सहित अश्लील सामग्रीसँग सम्बन्धित सबै कुराहरू समावेश गर्दछ।

५) फिसिङ - क्रेडिट कार्ड नम्बरहरू, खाता प्रयोगकर्ता नामहरू, पासवर्डहरू, सामाजिक सुरक्षा नम्बरहरू, इत्यादि जस्ता व्यक्तिगत डेटाहरू प्रकट गर्न अन्त-प्रयोगकर्ताहरूलाई छल गर्ने उद्देश्यले भ्रामक वेबसाइटहरू। यी वेबसाइटहरूले बैंकहरू जस्ता सामान्य, प्रख्यात साइटहरू भएको बहाना गर्छन्। क्रेडिट कार्ड कम्पनीहरु।

६) सामाजिक सञ्जाल।डेटिङ - फोरम, च्याट, इमेल वा अन्य विधिहरू मार्फत अन्तरक्रिया, डेटिङ वा अन्य नेटवर्किङ प्रवर्द्धन गर्ने निःशुल्क वा सशुल्क सेवाहरू प्रदान गर्ने साइटहरू।

७) असहिष्णुता।अतिवाद - यो वर्गले आतंकवादी गतिविधि वा अतिवादको वकालत गर्ने कुनै पनि साइटलाई जनाउँछ। यसमा भेदभाव वा जातीय भेदभावमा आधारित व्यक्ति र।वा समूहहरूप्रति चरम राजनीतिक विचार र असहिष्णुता भएका समूहहरू समावेश छन्।

८) स्पाइवेयर।एडवेयर - वेबसाइटहरू जसले अनावश्यक विज्ञापनहरू प्रदर्शन गर्दछ वा प्रयोगकर्ताको जानकारी बिना प्रयोगकर्ताको बारेमा जानकारी सङ्कलन गर्ने कोडहरू वितरण गर्न वा समावेश गर्न चिनिन्छ।

९) एनोनिमाइजर - यो वर्गले साइटहरूलाई बुझाउँछ जसले प्रयोगकर्तालाई अज्ञात रूपमा नेट सर्फ गर्न अनुमति दिन्छ। यसले साइटहरूलाई पनि बुझाउँछ जसले प्रयोगकर्तालाई बेनामी इमेलहरू पठाउन अनुमति दिन्छ। यसमा प्रोक्सी बाइपास जानकारी वा सेवाहरू प्रदान गर्ने साइटहरू पनि समावेश छन्।

१०) प्रतिलिपि अधिकार उल्लङ्घन - यो वर्गले मिडिया, सफ्टवेयर, एमपि३, डिभिडि चलचित्रहरू वा अन्य कुनै पनि प्रतिलिपि अधिकार सामग्रीहरू प्रदान गर्ने साइटहरूलाई बुझाउँछ जुन खरिद वा डाउनलोडको लागि अवैध रूपमा उपलब्ध छ। बुटलेग्ड सफ्टवेयरको डाउनलोड र स्थापनाको कारणले गर्दा आइप्रसम मालिकहरूलाई दायित्वबाट जोगाउन यो वर्ग प्रायः अवरुद्ध हुन्छ। ध्यान दिनुहोस कि यो श्रेणीले कम्प्युटर ह्याकिङका लागि विशिष्ट साइटहरूलाई सन्दर्भ गर्दैन।

११) नग्नता - यो वर्गले नग्नताको छवि वा प्रतिनिधित्व प्रदान गर्ने साइटहरूलाई जनाउँछ। तिनीहरू कलात्मक वा गैर-कलात्मक रूपमा हुन सक्छन जस्तै पत्रिकाहरू, चित्रहरू, चित्रहरू, मूर्तिकलाहरू, इत्यादि। यो श्रेणी ती साइटहरूलाई तोकिएको छ जुन दुवै आंशिक र पूर्ण नग्नता प्रदर्शन गर्दछ यद्यपि छविहरू अश्लील प्रकृतिको नहुन सक्छ।

१२) मालवेयर - प्रयोगकर्ताको ज्ञान बिना प्रयोगकर्ताको प्रणाली परिमार्जन गर्न सक्ने हानिकारक कोड समावेश गर्ने वेबसाइटहरू।

१३) स्थानीय अस्वीकार - यी वेबसाइटहरू हुन जुन पहिचान गरिएको छ तर माथि पहिचान गरिएका कोटिहरू मध्ये एकमा पर्दैन।

ii. आइएमएनटि ले आवधिक रूपमा प्रवृति रिपोर्टको समीक्षा गर्नेछ र के अवरुद्ध वा फिल्टर गरिएको छ आवश्यकता अनुसार समायोजन गर्नेछ।

१) सबै प्रयोगकर्ताहरूलाई जिल्लाको शैक्षिक, शिक्षण, प्रशासनिक, व्यापार, वा समर्थन सेवा उद्देश्यहरू प्रवर्द्धन नगर्ने वा कुनै निर्देशन, परियोजना, जागिर, कार्य असाइनमेन्टसँग सम्बन्धित नभएको इन्टरनेटको अंशहरू जानीजानी पहुँच गर्न वा पहुँच गर्न प्रयास गर्न निषेध गरिएको छ। , कार्य, वा कार्य जसको लागि प्रयोगकर्ता जिम्मेवार छ।

२) जिल्ला सञ्जालको कुनै पनि प्रयोगकर्ता जसले इन्टरनेटको कुनै अंश पहिचान गर्छ जसमा प्रविधि संरक्षण उपाय मार्फत फिल्टर नगरिएको अनुपयुक्त सामग्री समावेश छ भने तुरुन्त हेल्प डेस्कमा सम्पर्क गर्नुपर्छ।

३) जिल्ला सञ्जालको प्रयोगकर्ताले ती स्रोतहरू व्यक्तिगत व्यावसायिक उद्देश्य वा व्यक्तिगत आर्थिक वा अन्य लाभको लागि प्रयोग गर्नु हुँदैन।

क) अन्य उद्देश्यका लागि जिल्ला नेटवर्कको आकस्मिक व्यक्तिगत प्रयोगलाई सुपरिटेन्डेन्ट वा नियुक्त व्यक्तिको विवेकमा अनुमति दिइएको छ जब प्रयोग:

i) ती स्रोतहरू अनावश्यक रूपमा उपभोग गर्दैन

ii) प्रयोगकर्ताको काम वा अन्य जिल्ला जिम्मेवारीहरूको प्रदर्शनमा हस्तक्षेप गर्दैन

iii) प्रयोगकर्ताको कामको समयको अनुचित मात्रा खपत गर्दैन;

iv) विद्यालय वा कामको वातावरणमा अनुपयुक्त विषयहरूको चिन्ता गर्दैन (जस्तै अश्लील वेब साइटहरू पहुँच गर्ने);

v) बालबालिकालाई सिकाउने जिल्लाको मिशनसँग असंगत छैन;

vi) अन्यथा लागू कानूनको अनुपालनमा छ, शिक्षा बोर्डको नीति र सुपरिटेन्डेन्टको नियमहरू; र

vi) प्रतिबन्धित जानकारी छैन। २. गोप्य र अन्य इलेक्ट्रोनिक जानकारीमा पहुँच

क. इ-मेल संचार वा संलग्नकहरूमा समावेश भएका विद्यार्थीहरूको बारेमा व्यक्तिगत रूपमा पहिचान योग्य जानकारी, विद्यार्थी शिक्षा रेकर्डहरूमा समावेश जानकारी, चिकित्सा जानकारी, र असक्षमताहरू बारे जानकारी पारिवारिक शैक्षिक अधिकार र गोपनीयता ऐन ("एफइआरपिए") र स्वास्थ्यको अनुपालनमा हुनुपर्छ। बीमा पोर्टेबिलिटी र एकाउन्टेबिलिटी एक्ट ("एचआइपिपिए")।

ख. जिल्ला कर्मचारीहरूले जिल्लाको इलेक्ट्रोनिक जानकारीमा पहुँच गर्न सक्छन बशर्ते कर्मचारीले कामको जिम्मेवारीहरू पूरा गर्न सामग्रीहरू पहुँच गर्न आवश्यक छ। पहुँच कार्य जिम्मेवारीहरू पूरा गर्न आवश्यक जानकारीमा सीमित हुनेछ।

ग. गैर-बिओई कर्मचारी र कर्मचारीहरूको लागि; पर्यवेक्षकहरू र अन्य जिल्ला कर्मचारीहरूले कुनै पनि वा सबै इ-मेल सन्देशहरू, कम्प्युटर फाइलहरू, वा कुनै पनि कर्मचारीले प्रयोग गरेको इलेक्ट्रोनिक डाटा समीक्षा गर्न, राख्न वा मेटाउन जिल्ला नेटवर्कमा जहाँसुकै भण्डारण गरिएको इलेक्ट्रोनिक जानकारी पहुँच गर्न सक्नेछन्। जानकारी जिल्लाको सामान्य काउन्सिल वा नियुक्ति र महालेखा परीक्षक द्वारा अनुमोदन गरिएको छ।

घ. बिओई कर्मचारी र कर्मचारीहरूका लागि, पर्यवेक्षक कर्मचारीहरूले कुनै पनि वा सबै इ-मेल सन्देशहरू, कम्प्युटर फाइलहरू, वा इलेक्ट्रोनिक डेटालाई कर्मचारीले प्रयोग गरेको अनुमति दिईएको कुनै पनि समयमा समीक्षा गर्न, राख्न वा मेटाउन जिल्ला नेटवर्कमा कहीं पनि भण्डारण गरिएको इलेक्ट्रोनिक जानकारी पहुँच गर्न सक्छन्। त्यो जानकारी पहुँच गर्न महालेखा परीक्षक द्वारा अनुमोदन गरिएको छ।

ङ. **प्रतिबन्धित जानकारी** र अनुमोदनहरूमा पहुँचको लागि सबै अनुरोधहरू दस्तावेज हुनुपर्छ। अनुरोधमा अनुरोधको कारण, अनुरोध गरिएको जानकारीको अवधि, र जानकारी प्राप्त गर्ने कुनै पनि अतिरिक्त पक्षहरू निर्दिष्ट गरिएको हुनुपर्छ। अनुलग्नक १ अनुरोध कागजात गर्न प्रयोग गर्नुपर्छ।

च. वित्तीय जानकारी, व्यक्तिगत जानकारी, विद्यार्थी, अभिभावक, कर्मचारी, वा व्यापार साझेदारहरू जसका लागि उनीहरूलाई अधिकार दीएको छैन, लगायतका जिल्ला सूचना र।वा **प्रतिबन्धित सूचनाहरू** कसैले पनि पहुँच वा खुलासा गर्ने छैनन्।

छ. बिओई को महालेखा परीक्षकको कार्यालयले रोचेस्टर सिटी स्कूल डिस्ट्रिक्ट भित्रका सबै प्रणाली, कागजातहरू र जानकारीहरूमा पूर्ण र असीमित पहुँच हुनेछ।

प्रयोगकर्ता (जिल्ला विद्यार्थीहरू बाहेक) द्वारा यस नीतिको कुनै पनि उल्लङ्घनले लागू हुने सामूहिक सौदाबाजी सम्झौता वा बोर्ड र सुपरिटेन्डेन्टको रोजगार नियम र नियमहरू, र लागू कानूनसँग सुसंगत पहुँच र अनुशासन अस्वीकार गर्न सक्छ। जिल्ला विद्यार्थीद्वारा यस नीतिको कुनै पनि उल्लङ्घनले आचार संहिता (नीति १४००) र लागू कानूनसँग सुसंगत पहुँच र अनुशासन अस्वीकार गर्न सक्छ।

अन्तर-संदर्भ: आचार संहिता (१४००)
स्कूल नेटवर्क स्वीकार्य प्रयोग (१९५०-आर)

नोटहरू: संकल्प नं. २०१०-११: ९०७ अनुसार जुन २२, २०११ ग्रहण गरिएको; संशोधन नम्बर २०१३-१४: ५१३ अनुसार फेब्रुअरी २८, २०१४; २०२२-२३: २०६ को संकल्प नं. अनुसार २० अक्टोबर २०२२ मा संशोधित