ISTITUTO COMPRENSIVO STATALE "CRONILDE MUSSO"
VIA ANDANTE 14 - 28069 TRECATE *(NO) Tel. 0321777788*
Cod. Ministeriale NOIC83000Q - E mail noic83000q@istruzione.it - E mail noic83000q@pecistruzione.it
Codice Fiscale 94068520033 - Codice univoco UFQMWC
Sito http://www.iccronildemusso.edu.it/

Regolamento sulla Politica di Uso Accettabile della rete (PUA)

Premessa e finalità

Il curricolo scolastico prevede il possibile utilizzo di strumentazioni informatiche (PC o dispositivi portatili) con cui gli studenti potranno svolgere le normali attività, trovare materiale, recuperare documenti e scambiare informazioni utilizzando le Tecnologie per l'Informazione e la Comunicazione (TIC).

Per gli studenti e per gli insegnanti l'accesso ad internet a scuola, nel rispetto delle disposizioni del Ministero dell'Istruzione Università e Ricerca che vietano l'uso in classe di telefoni cellulari e dispositivi elettronici, è consentito esclusivamente per uso didattico.

La presente Politica per l'Uso Accettabile della rete della scuola, fornisce le linee guida per il benessere e la sicurezza di tutti gli utenti della rete.

CAPITOLO 1 – Comportamenti

Comportamento in rete e uso consapevole delle Tecnologie

Con l'avvento del web 2.0 e dei Social Network, basati sui principi di collaborazione e condivisione diretta degli utenti, internet e i suoi servizi si sono evoluti, dando vita ad una serie di principi di buon comportamento del web2.0 che prende il nome di **Netiquette 2.0.**

Questi principi sono le linee guida fondamentali per la sicurezza e il benessere di tutti nella rete, in particolare negli ambienti più usati dagli adolescenti. Tutti gli utenti della rete dell'Istituto devono rispettare scrupolosamente questi principi, le leggi vigenti in materia di diritto d'autore e tutela della privacy nonché le specifiche norme penali relative al settore informatico e della comunicazione elettronica, oltre ad ogni altra disposizione generale di legge.

Principi Generali

1. Internet favorisce la libertà d'espressione, ma è necessario sapere che ci sono contenuti illeciti.

2. Quando si inizia a navigare tra i servizi dei Social Network e le applicazioni web tipo YouTube, Facebook, Instagram, Twitter, WhatsApp, Telegram, Netlog, etc…, bisogna informarsi su quali sono i diritti e i doveri dell'utente, leggendo il regolamento, tenendosi aggiornati.

3. Se si condividono informazioni personali, bisogna farlo scegliendo con cura che cosa rendere pubblico e cosa rendere privato, scegliendo con cura le amicizie e i gruppi a cui aderire e proteggendo

la propria identità digitale con password complesse e usando una domanda di recupero password dalla risposta non banale (evitare nomi del proprio cane, gatto, ecc…).

4. Se si condividono elementi multimediali o informazioni che riguardano più persone è necessario avere il permesso di ciascun utente coinvolto prima di effettuare la pubblicazione. Non bisogna pubblicare sui social media foto e/o video fatti di nascosto e dove sono presenti persone filmate senza il loro consenso.

5. Bisogna contribuire a rendere il Web un luogo sicuro, pertanto ogni volta che un utente commette involontariamente un abuso o un errore, pubblicando del materiale illecito, non idoneo o offensivo, bisogna contattarlo e fornire le spiegazioni relative alle regole, diffondendo così i principi della sicurezza.

6. Ogni abuso subito o rilevato nella navigazione, deve essere segnalato tramite i canali e gli strumenti offerti dal servizio indicando in modo semplice i riferimenti per ottenere tempestivamente la rimozione del contenuto (abuso, data, ora, utenti e servizio coinvolti). Tutti i social network garantiscono la possibilità di segnalare materiale inopportuno mediante semplici operazioni da compiere direttamente sul sito.

<u>Comportamenti nelle relazioni tra persone</u>

1. All'interno dei Social Network si instaurano tante relazioni tra singoli utenti, non veicolate o controllate da intermediari, chiamati rapporti di pari livello. È importante fare attenzione a quali informazioni vengono fornite in questo contesto, evitando di condividere dati personali e di contatto, come numeri di telefono o indirizzi, che nella vita reale non si darebbero a persone che non sono ancora degne di fiducia.

2. Bisogna evitare di scambiare file con utenti di cui non ci si può fidare e in ogni caso, anche quando si conosce l'interlocutore, è necessario verificare sempre l'origine dei file ed effettuarne un controllo con un antivirus aggiornato.

3. Se durante una chat, un forum o una qualsiasi discussione online, l'interlocutore diviene volgare, offensivo o minaccioso, si deve evitare di fomentarlo, ignorandolo e abbandonando la conversazione.

4. Quando si riscontra un comportamento riconducibile ad un illecito durante una conversazione privata, per esempio un tentativo di approccio sessuale nonostante la minore età, stalking o cyberbullismo, l'utente può sfruttare gli appositi sistemi di reportistica degli abusi predisposti all'interno del servizio, segnalando tempestivamente il nickname che ha perpetrato l'abuso. In questi casi può essere conveniente abbandonare non soltanto la conversazione ma anche il profilo personale usato fino a quel momento creandosene uno nuovo.

5. E' importante evitare di scaricare dei file che possono essere considerati illegali e protetti dal diritto d'autore. Bisogna inoltre fare attenzione e non aprire mai dei file sospetti, verificandone la bontà con un antivirus aggiornato.

6. I sistemi di messaggistica dei Social Network hanno le stesse regole della posta elettronica quindi è necessario preservare la privacy di tutti, cancellando il mittente o i vari destinatari quando si invia un messaggio a più destinatari che non si conoscono tra loro.

7. Quando si scambiano contenuti multimediali o si pubblicano video con colonna sonora o musica di sottofondo bisogna essere sicuri di averne il diritto d'uso e di non utilizzare alcun file coperto da copyright.

Creazione e diffusione di contenuti generati dagli utenti

1. I contenuti pubblicati sulle applicazioni web dei Social Network, hanno diversi livelli di visibilità, per esempio singoli utenti o tutti gli utenti della rete, pertanto, quando si inizia a pubblicare materiale in una community bisogna studiare ed imparare ad utilizzare correttamente le funzioni per l'impostazione dei livelli di privacy.

2. Dal momento che ciò che viene pubblicato su un Social Network è persistente e spesso non è facile da cancellare, bisogna evitare di contribuire con materiale che in futuro non si vorrebbe veder pubblicato.

3. Quando si contribuisce con del materiale in un ambiente condiviso, l'utente è tenuto ad essere coerente con il contesto e le regole di fatto della community, evitando di pubblicare materiale inadeguato e che potrebbe risultare fuori contest.

4. Se un contenuto viene moderato e non è più visibile online, probabilmente è non idoneo. Modificare linguaggio e controllare se il punto dove lo si è pubblicato è davvero il posto migliore per quello specifico contenuto.

5 Quando si fa uso di etichette(TAG) per catalogare un contenuto/utente, bisogna assicurarsi che sia coerente con il contenuto o che indichi la persona corretta; quando il TAG riguarda una persona sarebbe inoltre opportuno contattarla preventivamente per ottenere il consenso a collegare l'identità della persona al contenuto.

Gestione delle relazioni sociali – Communities

1. Le relazioni sociali che si sviluppano all'interno di un Social Network sono simili a quelle reali: deve essere gestita la fiducia verso i propri contatti proprio come accade nella realtà.

2. Se si instaura un'amicizia virtuale con persone di cui non si conosce la reale identità, bisogna evitare di condividere contatti e dati personali e contenuti privati, soprattutto se riguardano terze persone.

3. La reputazione digitale è persistente e si diffonde velocemente pertanto non bisogna mai diffamare altre persone, soprattutto se le stesse non sono presenti sul Social Network e non possono accorgersi del danno subito.

CAPITOLO 2 – Sicurezza e Uso delle TIC

Rete di Istituto, servizi e postazioni informatiche

Sicurezza nell'uso delle TIC nei Laboratori e nelle Postazioni per Docenti e Studenti

Al fine di garantire una gestione il più possibile corretta, la scuola attua le seguenti strategie:

▪ Il Dirigente Scolastico si riserva, sentiti i responsabili, di limitare l'accesso e l'uso della rete interna (Intranet) ed esterna (Internet) secondo i normali canali di protezione presenti nei sistemi operativi e utilizzando, se necessario, software/hardware aggiuntivi come Firewall;

E' FATTO DIVIETO DI:

▪ Scaricare file video-musicali protetti da copyright

▪ Visitare siti non necessari ad una normale attività didattica

▪ Alterare i parametri di protezione dei computer in uso

▪ Utilizzare la rete per interessi privati e personali che esulano dalla didattica

▪ Non rispettare le leggi sui diritti d'autore

▪ Navigare su siti non accettati dalla protezione interna alla scuola.

Disposizioni, comportamenti, procedure:

▪ Il sistema informatico è periodicamente controllato dai responsabili

▪ La scuola può controllare periodicamente i file utilizzati, i file temporanei e i siti visitati da ogni macchina

▪ È vietato installare e scaricare da Internet software non autorizzati

▪ Le postazioni PC in ambiente Windows sono protette da software che impedisce modifiche ai dati memorizzati sul disco fisso interno

▪ Al termine di ogni collegamento la connessione deve essere chiusa

▪ L'utilizzo di CD, chiavi USB e dispositivi removibili personali deve essere autorizzato dal docente e solo previa scansione antivirus

▪ La scuola si riserva di limitare il numero di siti visitabili e le operazioni di download

Utilizzo dei servizi Internet

▪ L'insegnante di classe, che ha nella propria programmazione l'utilizzo di Internet, è responsabile di quanto avviene nelle proprie ore di laboratorio;

▪ È vietato utilizzare e-mail personali ad uso privato durante le ore di lezione

▪ È vietato l'utilizzo delle postazioni durante le ore di lezione per motivi non strettamente legati alla pratica didattica;

▪ Gli allievi non possono usare dispositivi informatici dell'Istituto o personali, nella rete internet, senza l'ausilio e il coordinamento del docente

▪ È vietato il download a fini personali di file musicali, foto, software, video, ecc., tranne nel caso di specifiche attività didattiche preventivamente programmate.

Sicurezza della rete interna (LAN)

L'Istituto dispone di un dominio su rete locale (rete segreteria) cui accedono i computer dell'amministrazione e di reti per i plessi scolastici (reti didattiche) distinte da quelle della segreteria La rete interna è protetta da Firewall per quanto riguarda le connessioni con l'esterno. Le postazioni sono protette con sistemi antivirus regolarmente aggiornati. Per quanto concerne la rete amministrativa, essa è garantita da backup automatico (disco fisso interno ed esterno, Cloud) per il salvataggio dati..

Linee guida di utilizzo delle TIC per Studenti e Docenti

Studenti

▪ Non utilizzate giochi né in locale, né in rete;

▪ Salvate sempre i vostri lavori (file) in cartelle personali e/o di classe sui dispositivi di memorizzazione esterni, su cloud (GoogleDrive, OneDrive, Dopbox, etc.) e non in posizioni sull'hard disk locale: le

postazioni dedicate alla didattica eliminano qualunque dato alla fine della sessione di lavoro, per ragioni di tutela e sicurezza

▪ Mantenete segreto il nome, l'indirizzo, il telefono di casa, il nome e l'indirizzo della vostra scuola

▪ Non inviate a nessuno fotografie vostre o di vostri amici

▪ Chiedete sempre al vostro insegnante il permesso di scaricare documenti da Internet;

▪ Chiedete sempre il permesso prima di iscrivervi a qualche concorso o prima di riferire l'indirizzo della vostra scuola;

▪ Riferite al vostro insegnante se qualcuno vi invia immagini che vi infastidiscono e non rispondete; riferite anche al vostro insegnante se vi capita di trovare immagini di questo tipo su Internet;

▪ Se qualcuno su Internet vi chiede un incontro di persona, riferitelo al vostro insegnante, comunque ad un adulto;

▪ Ricordatevi che le persone che incontrate nella rete sono degli estranei e non sempre sono quello che dicono di essere;

▪ Non è consigliabile inviare mail personali, perciò rivolgetevi sempre al vostro insegnante prima di inviare messaggi di classe;

▪ Non caricate o copiate materiale da Internet senza il permesso del vostro insegnante

Docenti

▪ Evitate di lasciare le e-mail o file personali sui computer o sul server della scuola, ~~lo spazio è limitato~~;

▪ Salvate sempre i vostri lavori (file) in cartelle personali e/o di classe sui dispositivi di memorizzazione esterni, su cloud (GoogleDrive, OneDrive, Dopbox, etc.) e non sull'hard disk locale: le postazioni dedicate alla didattica eliminano qualunque dato alla fine della sessione di lavoro, per ragioni di tutela e sicurezza;

▪ Discutete con gli alunni della PUA (Politica d'Uso Accettabile) della scuola e degli eventuali problemi che possono verificarsi nell'applicazione delle regole relative all'uso di Internet;

▪ Date chiare indicazioni su come si utilizza Internet, ed eventualmente anche la posta elettronica, e informateli che le navigazioni saranno monitorate;

▪ Ricordate di verificare lo stato dei computer alla fine della sessione di lavoro, in particolare controllando che siano tutti spenti all'uscita dall'ultima ora di lezione;

▪ Ricordate agli alunni che le infrazione saranno sanzionate in riferimento al Regolamento di Istituto e alla normative vigente

Sito web dell'Istituto

L'Istituto dispone di un proprio spazio web e di un proprio dominio: www.iccronildemusso.edu.com

Le informazioni pubblicate sul sito della scuola relative alle persone da contattare rispetteranno le norme vigenti sulla privacy.

Approvato dal Consiglio di Istituto nella seduta del 27 marzo 2020