E-Safety Policy

I.C. MATTEO RICCI

INDICE RAGIONATO

1. Introduzione

- Scopo della Policy.
- Ruoli e Responsabilità (*che cosa ci si aspetta da tutti gli attori della Comunità Scolastica*).
- Condivisione e comunicazione della Policy all'intera comunità scolastica.
- Gestione delle infrazioni alla Policy.
- Monitoraggio dell'implementazione della Policy e suo aggiornamento.
- Integrazione della Policy con Regolamenti esistenti.

2. Formazione e Curricolo

- Curricolo sulle competenze digitali per gli studenti.
- Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica.
- Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
- Sensibilizzazione delle famiglie.

3. Gestione dell'infrastruttura e della strumentazione ICT della scuola.

- Accesso ad internet: filtri antivirus e sulla navigazione.
- Gestione accessi (password, backup, ecc.).
- E-mail.
- Blog e sito web della scuola
- Protezione dei dati personali.

4. Strumentazione personale

- Per gli studenti: gestione degli strumenti personali - cellulari, tablet ecc..
- Per i docenti: gestione degli strumenti personali - cellulari, tablet ecc..
- Per il personale della scuola: gestione degli strumenti personali - cellulari, tablet ecc..

5. Prevenzione, rilevazione e gestione dei casi

Prevenzione

- Rischi
- Azioni

Rilevazione

- Che cosa segnalare
- Come segnalare: quali strumenti e a chi.
- Come gestire le segnalazioni.

Gestione dei casi

- Definizione delle azioni da intraprendere a seconda della specifica del caso.

Cap. 1 INTRODUZIONE

Nell'era dell'informazione le nuove tecnologie hanno mutato la società in maniera radicale e irreversibile e l'interconnessione di tutti i computer del pianeta influenza ogni settore della vita umana. I bambini entrano in contatto col mondo informatico da subito risultandone affascinati e mostrando di sapervisi muovere con naturalezza e senza preconcetti, esponendosi però a rischi importanti. Una scuola che ignorasse tutto questo sarebbe anacronistica, pertanto il nostro Istituto Comprensivo ha intrapreso un percorso finalizzato ad offrire alle nuove generazioni quegli strumenti indispensabili a governare attivamente la realtà odierna aprendosi all'uso delle TIC nella didattica, ma tenendo anche conto dei pericoli che il cyberspazio cela in sé.

1.1 SCOPO

L'idea di una policy di e-safety, strumento di regolamentazione, monitoraggio e condivisione di comportamenti, sanzioni e attività, trae ispirazione dall'adesione al progetto del MIUR *Generazioni Connesse* (www.generazioniconnesse.it), al quale il nostro Istituto Comprensivo ha scelto di aderire nell'anno scolastico 2017 – 2018, avvertendo l'esigenza di prevenire e contrastare il fenomeno del Cyber Bullismo in virtù delle iniziative digitali intraprese e della volontà di alimentare la politica di inclusione e apertura verso l'altro che ci contraddistingue.

1.2 RUOLI E RESPONSABILITÀ

Tutti gli attori della comunità scolastica sono coinvolti in prima persona e pertanto chiamati in causa nell'assunzione di proprie specifiche responsabilità.

RUOLI	RESPONSABILITÀ
Dirigente Scolastico	• Presentare la policy al Collegio dei Docenti e al Consiglio di Istituto; • Garantire la formazione dei docenti sull'uso delle TIC nella didattica e dell'uso sicuro di Internet e della rete. • Garantire l'esistenza di un sistema di monitoraggio e controllo della sicurezza on line in collaborazione con personale scolastico, enti locali e enti territoriali interessati. A tale scopo necessita di ricevere tempestive informazioni sulle violazioni al presente regolamento o eventuali problemi attualmente non noti dal corpo docente o dal personale ATA che ne vengano a conoscenza.
Direttore dei Servizi Generali e Amministrativi	• Assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento dei tecnici per garantire una infrastruttura tecnica funzionante, sicura e non aperta a usi impropri o ad attacchi esterni. • Garantire il funzionamento dei diversi canali di comunicazione della scuola (sito web, circolari, sportello di

	ascolto…).
Responsabile della sicurezza on line (nominato dal DS)	• Assicurarsi che tutti i docenti siano a conoscenza delle procedure di sicurezza on line • Essere a disposizione di tutti gli attori della scuola con lo scopo di prevenire, educare e contrastare il fenomeno del cyber bullismo • Funzionare da raccordo tra i docenti, le famiglie e il dirigente scolastico in caso di abusi tra studenti • In collaborazione con l'Animatore Digitle e il Team per l'innovazione, curare la redazione e la revisione annuale della policy sulla base delle osservazioni ricevute da tutti i soggetti interessati.
Animatore digitale e team per l'innovazione	• Assicurare la massima diffusione dentro la comunità scolastica in tutte le sue componenti (docenti/ata, genitori e studenti), mediante pubblicazione sul sito della scuola. • Accertarsi che la policy sia pubblicata sul sito web della scuola • Monitorare l'uso corretto delle attrezzature digitali e il loro funzionamento • Veicolare informazioni relative a progetti e azioni in collaborazione con il responsabile della sicurezza on line e della Fs Formazione, Aggiornamento e Tecnologie. • Relazionarsi con la ditta che gestisce l'assistenza tecnico-informatica per definire le misure di sicurezza informatica più opportune; riferire al Dirigente Scolastico situazioni o problemi di particolare rilevanza su cui intervenire
FS Formazione, Aggiornamento e Tecnologie	• Promuovere attività laboratoriali di educazione socio-affettiva rivolte agli studenti. • Proporre corsi di formazione relativi all'uso corretto di software ed hardware in dotazione all'istituto, ma anche al fenomeno del cyberbullismo.
Personale docente con particolare riferimento ai Coordinatori dei Consigli di Classe	• Avere adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto e relative buone pratiche; • Aver letto, compreso e sottoscritto la presente policy; • Illustrare il presente documento ai propri alunni invitandoli a rispettarne il regolamento • Segnalare al team digitale, attraverso apposita relazione

	scritta, eventuali malfunzionamenti delle attrezzature informatiche in dotazione. • Segnalare comportamenti di abuso compiuti dagli studenti informandone il responsabile della prevenzione al cyberbullismo attraverso la compilazione dell'apposito modulo modulo • Non salvare file contenenti dati personali sui dispositivi della scuola • Controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche ecc. nelle lezioni e nelle altre attività scolastiche che ne prevedono la necessità a scopi didattici; • Guidare la navigazione di studentesse e studenti, nelle lezioni in cui l'uso di Internet è pianificato, verso siti controllati come idonei per il loro uso, onde evitare di incontrare materiali inadatti • Far nascere negli alunni una buona cognizione della proprietà del software e delle normative sul diritto d'autore nonché di far comprendere la necessità di effettuare ricerche sul web e la relativa estrazione di documenti evitando il plagio o l'illecita diffusione di dati personali; • non divulgare le credenziali di accesso agli account (username e password) e/o, nel caso ne sia a conoscenza, alla rete wi-fi; • non allontanarsi dalla postazione lasciandola incustodita, se non prima di avereffettuato la disconnessione;
Personale scolastico (ATA)	• Conoscere le norme della policy, contribure alla sorveglanza e intervenire di fronte a comportamenti scorretti informandone il responsabile attraverso la compilazione di un modulo
Alunni	• Rispettare le indicazioni della policy per un uso corretto delle TIC • Adottare condotte rispettose dell'altro, anche durante le comunicazioni in rete • Conoscere il protocollo e denunciare comportamenti pericolosi e scorretti, anche mantenendo l'anonimato. • Non utilizzare dispositivi personali durante le attività didattiche se non espressamente consentito dal personale docente • Avere una buona comprensione delle possibilità di ricerca sul web e della necessità di evitare il plagio, rispettare le normative sul diritto d'autore, non diffondere dati personali • Conoscere e comprendere le politiche sull'uso di dispositivi mobili e di macchine fotografiche digitali • Capire l'importanza di adottare buone pratiche di sicurezza

	informatica in tutti i momenti della vita, a tutela dell'incolumità propria e altrui e per evitare di perpetrare reati punibili sia a livello scolastico sia da parte della magistratura. • Non utilizzare la strumentazione della scuola per scopi personali, ludici e/o ricreativi, a meno che l'attività didattica non lo preveda esplicitamente
Genitori	Genitori e tutori svolgono un ruolo cruciale nel garantire che i loro figli comprendano la necessità di utilizzare i dispositivi Internet e mobili in modo appropriato. La scuola coglierà ogni occasione per sensibilizzare i genitori circa questi problemi attraverso incontri con la Polizia municipale ed altri esperti o educatori, circolari, sito web e altre comunicazioni telematiche, informazioni su campagne di sicurezza promosse da altre istituzioni o su convegni dedicati a questo tema. • Prendere visione della policy contribuendo a sensibilizzare ed educare i ragazzi ad un uso sicuro e corretto delle TIC e al rispetto verso l'altro • Sostenere la politica della scuola in merito all'uso delle TIC nella didattica • Firmare il patto di corresponsabilità.

1.3 CONDIVISIONE E COMUNICAZIONE DELLA POLICY ALL'INTERA COMUNITÀ SCOLASTICA.

All'inizio dell'anno scolastico tutti gli attori della comunità scolastica saranno messi al corrente dell'esistenza della policy di e-safety e dei suoi contenuti attraverso le seguenti azioni:

- pubblicazione della policy sul sito web scolastico;
- presentazione della policy in Collegio Docenti e Consiglio di Istituto;
- firma del patto di corresponsabilità da parte delle famiglie;
- assunzione delle proprie responsabilità educative da parte di tutto il personale dell'istituto comprensivo.

1.4 GESTIONE DELLE INFRAZIONI ALLA POLICY.

Se ad infrangere la policy - con l'inosservanza delle regole di gestione dei materiali digitali o di mancato intervento di fronte a infrazioni realizzate dagli alunni - è un docente o un altro componente del personale scolastico i provvedimenti presi saranno quelli previsti dal contratto di lavoro.
Qualora le infrazioni vengano compiute dagli studenti, sarà invece compito del consiglio di classe decidere la sanzione più opportuna tenendo conto del tipo di infrazione commessa e dell'età dell'autore dell'illecito. I provvedimenti disciplinari potranno realizzarsi attraverso:

- un richiamo verbale;

- una nota sul diario;
- la convocazione dei genitori per un colloquio con gli insegnanti o gli insegnanti e il DS;
- dei lavori socialmente utili;
- una sospensione con obbligo di frequenza.

1.5 MONITORAGGIO DELL'IMPLEMENTAZIONE DELLA POLICY E SUO AGGIORNAMENTO.

Durante l'anno scolastico i docenti testimoni di infrazioni da parte di studenti saranno tenuti a compilare un modulo di segnalazione dell'illecito. Nel mese di giugno la commissione cyberbullismo sotto la supervisione del DS si riunirà per analizzare le problematiche emerse e le modalità adottate per gestirle sulla base delle segnalazioni, delle infrazioni e delle sanzioni adoperate; se ritenuto necessario la commissione provvederà a modificare e migliorare la policy.

1.6 INTEGRAZIONE DELLA POLICY CON REGOLAMENTI ESISTENTI.

Questo documento si integra con il PTOF, IL PDM, il regolamento di istituto, la policy sulla privacy e la normativa vigente, didattica e non, in paricolar modo con la legge n. 71/2017, il PNSD, la carta dei doveri e dei diritti in Internet (2015).

Cap. 2 FORMAZIONE E CURRICOLO

2.1 CURRICOLO SULLE COMPETENZE DIGITALI PER GLI STUDENTI.

La scuola Matteo Ricci fa riferimento al modello nazionale della certificazione delle competenze previste al termine del primo ciclo di Istruzione:

[Lo studente] *ha buone competenze digitali, usa con consapevolezza le tecnologie della comunicazione per ricercare e analizzare dati ed informazioni, per distinguere informazioni attendibili da quelle che necessitano di approfondimento, di controllo e di verifica e per interagire con soggetti diversi nel mondo* - Indicazioni nazionali per il curricolo 2012

2.2 FORMAZIONE DEI DOCENTI SULL'UTILIZZO E L'INTEGRAZIONE DELLE TIC NELLA DIDATTICA.

Le attività di formazione si svolgeranno su due livelli:
· Formazione istituzionale, organizzata dal Miur secondo il PNSD, attraverso gli snodi formativi;
· Formazione specifica di Istituto, legata alle esigenza formative rilevate ad inizio d'anno dal Collegio Docenti;
All'inizio di ogni anno scolastico la Funzione Strumentali Tecnologie e Formazione, valutato a quali progetti/iniziative aderire e quali attività svolgere durante l'anno in corso, presenterà le sue proposte al Collegio Docenti per l'approvazione e la condivisione.

2.3 FORMAZIONE DEI DOCENTI SULL'UTILIZZO CONSAPEVOLE E SICURO DI INTERNET E DELLE TECNOLOGIE DIGITALI

Al fine di promuovere la condivisione di buone pratiche per un uso consapevole e sicuro delle ICT, e di prevenire e contrastare "ogni forma di discriminazione e del bullismo, anche informatico" (Legge 107/2015, art. 1, c. 7, l), il nostro Istituto ha aderito, quest'anno, al progetto "**Generazioni Connesse**" , coordinato dal MIUR, in partenariato col Ministero dell'Interno-Polizia Postale e delle Comunicazioni e con altre importanti associazioni per la tutela dei diritti dei minori, come Children Italia e Telefono Azzurro.

2.4 SENSIBILIZZAZIONE DELLE FAMIGLIE.

Il nostro istituto ha organizzato incontri aperti alle famiglie e agli studenti con enti esterni, come il Commissariato di zona e Telefono Azzurro, per sensibilizzare docenti, alunni e genitori sui temi della sicurezza online. Anche nei prossimi anni si continuerà ad utilizzare questo approccio per la sensibilizzazione delle famiglie, con incontri che offriranno occasione di confronto e discussione sui rischi rappresentati dall'uso di cellulari, smartphone e chat line senza un'adeguata formazione in merito ai rischi derivanti da un uso inappropriato di tali dispositivi. Sul sito scolastico saranno resi accessibili i materiali tratti del sito di "Generazioni connesse".

La scuola darà inoltre ampia diffusione, tramite pubblicazione sul sito, del presente documento di policy per consentire alle famiglie una piena conoscenza del regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e favorire un'attiva collaborazione tra la scuola e le famiglie sui temi della prevenzione dei rischi connessi a un uso inappropriato del digitale.

Cap. 3 GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE ICT DELLA SCUOLA

Attualmente il nostro Istituto è interamente connesso ad internet tramite cablaggio ethernet.
La Dirigenza e l'Amministrazione hanno una rete separata.
Gli alunni potranno usufruire della connessione solo tramite i pc dei laboratori di informatica con software di controllo gestito dal docente, ma ancora da installare).
Strumentazione ICT dell'Istituto:

- Laboratorio informatico Scuola Primaria Plesso Cina
- Laboratorio informatico Scuola Primaria Plesso Albacini
- Aula Multimediale Plesso Sabatini
- Laboratorio informatico Plesso Sabatini
- Atelier creativo Plesso Sabatini

3.1 ACCESSO AD INTERNET: FILTRI ANTIVIRUS E SULLA NAVIGAZIONE.

Nei laboratori di informatica e nelle aule dal prossimo anno scolastico saranno attivi filtri per la navigazione sicura, tramite gestione di blacklist, ed è inoltre prevista l'attivazione di software per

la gestione e il controllo delle postazioni. Le impostazioni sono definite e manutenute dall'Animatore digitale e dai responsabili di laboratorio ed è in carico a ciascun docente la segnalazione di malfunzionamenti e disservizi.
I docenti, nell'ambito della propira autonomia, hanno piena RESPONSABILITA' nel collegamento ai siti web nelle postazioni a loro riservate.
Occorre, inoltre, sensibilizzare tutta la comunità scolastica sull'opportunità di mantenere aggiornati gli antivirus installati sulle macchine personali e controllare i dispositivi di archiviazione esterna che vengano collegati al proprio pc.

3.2 GESTIONE ACCESSI (PASSWORD, BACKUP, ECC.).

Nei computer presenti nelle aule e nei laboratori sono previsti due profili di accesso con password relative:

- docente;
- alunno.

È possibile effettuare installazioni e aggiornamenti di software solo tramite la password di amministratore, fornita al personale di assistenza tecnica e all'Animatore Digitale.

Ciascun utente connesso alla rete dovrà rispettare il presente regolamento e la legislazione vigente, la propria privacy, quella degli altri utenti adulti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni elettroniche cui ha accesso e rispettare la cosiddetta netiquette (insieme di regole, comunemente accettate e seguite da quanti utilizzano Internete i servizi di rete, che disciplinano il comportamento di un utente nel rapportarsi agli altri utenti attraverso risorse come wiki, newsgroup, mailing list, forum, blog o e-mail).
I genitori saranno invitati a firmare e restituire un modulo di consenso. La componente studentesca dovrà impegnarsi a rispettare le norme di buon utilizzo che la scuola si impegna a redigere e a divulgare prima che sia concesso l'accesso a Internet.

3.3 E-MAIL.

L'account di posta elettronica è solo quello istituzionale utilizzato ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita. Le credenziali sono in possesso del personale amministrativo.
Le comunicazioni tra personale scolastico e famiglie via e-mail devono avvenire preferibilmente tramite l'indirizzo e-mail della scuola o all'interno della piattaforma di apprendimento (DA REALIZZARE), per consentire l'attivazione di protocolli di controllo.
I docenti utilizzano per scopi didattici il proprio account su dominio *istruzione.it*.
La posta elettronica è protetta da antivirus e da antispam.

3.4 SITO WEB DELLA SCUOLA.

La scuola ha un sito web gestito esternamente (http://www.icmatteoricci.gov.it/).
Il sito si configura come un'area pubblica per le informazioni che non comportano la diffusione di dati personali o riservati, in cui sono reperibili le informazioni sulla vita scolastica, iniziative e scadenze ministeriali e avvisi di carattere generale
Ogni pubblicazione avviene sotto diretta supervisione del Dirigente Scolastico che ne valuta la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy, ecc.

3.5 PROTEZIONE DEI DATI PERSONALI.

Si fa riferimento a tutto quanto previsto dal Decreto legislativo 30 giugno 2003, n. 196 (c. d. Codice della Privacy).

In particolare:

- Il personale scolastico è "incaricato del trattamento" dei dati personali (degli alunni, dei genitori, ecc.), nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione).
- Tutto il personale incaricato riceve poi istruzioni particolareggiate applicabili al trattamento di dati personali su supporto cartaceo e su supporto informatico, ai fini della protezione e sicurezza degli stessi.
- Viene inoltre fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori.
- La scuola cercherà di utilizzare fotografie o video di gruppo piuttosto che foto integrali di singoli.

Cap. 4 STRUMENTAZIONE PERSONALE

4.1 PER GLI STUDENTI: GESTIONE DEGLI STRUMENTI PERSONALI - CELLULARI, TABLET ECC…

Nell'Istituto non è consentito agli alunni l'uso di telefoni cellulari.
In caso di urgenza per comunicazioni tra gli alunni e le famiglie, su autorizzazione dei docenti e sotto il diretto controllo dei collaboratori scolastici, gli alunni potranno comunicare con le famiglie tramite gli apparecchi telefonici della scuola ; allo stesso modo le famiglie devono chiamare il centralino della scuola se hanno assoluta necessità di parlare con i propri figli. In ogni caso le comunicazioni devono avvenire solo in caso di inderogabile necessità e urgenza.
Gli studenti dotati dai propri genitori di un apparecchio telefonico sono pertanto tenuti a tenerli spenti e a depositarli, all'ingresso in aula e prima dell'appello, nelle apposite cassette collocate in aula durante l'intero orario delle lezioni.
Il corpo docente potrà valutare l'uso di dispositivi elettronici nell'ambito di attività didattiche programmate..
Individui con disturbi specifici di apprendimento, previa consultazione con il Consiglio di Classe, concorderanno le modalità di impiego di strumenti compensativi quali tablet e computer portatili e le modalità di custodia degli stessi.
E' vietato portare nelle aule dispositivi che possono avere accesso a Internet non filtrato (Sony Playstation, Microsoft Xbox e similari).
In caso contrario, saranno requisiti dal docente che ravvisa l'infrazione, depositati in dirigenza e consegnati al genitore/tutore convocato, che sarà contestualmente informato dell'eventuale sanzione disciplinare comminata al trasgressore.

L'invio di materiali abusivi, offensivi o inappropriati è vietato, anche se avviene all'interno di cerchie o gruppi di discussione privati
Le stesse regole saranno applicate durante uscite didattiche; caso per caso, saranno valutati modi e tempi di utilizzo di telefoni cellulari e altri dispositivi elettronici.
In ogni caso, gli studenti e le loro famiglie saranno ritenuti personalmente responsabili di tali dispositivi e dell'impiego degli stessi.

4.2 PER I DOCENTI: GESTIONE DEGLI STRUMENTI PERSONALI - CELLULARI, TABLET ECC…

Durante le ore di lezione è consentito ai docenti l'uso di dispositivi elettronici personali, unicamente a scopo didattico e a integrazione dei dispositivi scolastici disponibili. Durante l'orario di servizio l'uso del cellulare è consentito solo per comunicazioni personali che rivestano carattere di urgenza, mentre l'uso di altri dispositivi elettronici personali è permesso per attività funzionali all'insegnamento.
Durante l'attività didattica ogni insegnante deve:

- dare indicazioni sul corretto utilizzo della rete, condividendo con gli studenti la netiquette e indicandone le regole;
- assumersi la responsabilità di segnalare prontamente e per iscritto eventuali malfunzionamenti o danneggiamenti;
- non salvare sulla memoria locale della postazione dell'Istituto file contenenti dati personali e/o sensibili.

Qualora si utilizzino a scuola dispositivi di archiviazione esterna di proprietà personale (chiavette usb, dischi fissi portatili) è bene controllare preventivamente che essi siano esenti da virus per evitare di danneggiare le attrezzature comuni.

4.3 PER IL PERSONALE DELLA SCUOLA: GESTIONE DEGLI STRUMENTI PERSONALI - CELLULARI, TABLET ECC…

Durante l'orario di servizio al restante personale scolastico l'uso del cellulare è consentito per comunicazioni personali urgenti, previa richiesta autorizzazione alla Dirigente Scolastica. L'uso di altri dispositivi elettronici personali è permesso solo per attività funzionali al servizio, e preventivamente autorizzato.

4.4 PER IL PERSONALE DOCENTE: GESTIONE E UTILIZZO DELLE DOTAZIONI DELL'ISTITUTO

Nell'Istituto è vigente un regolamento di fruizione e di utilizzo delle dotazioni scolastiche, allegato alla presente. Si riporta un estratto delle disposizioni principali:
1. Le apparecchiature presenti nella scuola sono patrimonio comune, quindi, vanno utilizzate con il massimo rispetto.
2. I laboratori informatici e le postazioni informatiche dell'istituto possono essere utilizzati esclusivamente per attività di insegnamento, funzionali all'insegnamento e di formazione del personale docente e non docente.
3. Quando un insegnante, da solo o in classe, usufruisce del laboratorio deve obbligatoriamente registrare il proprio nome e l'eventuale classe nell'apposito registro delle presenze di laboratorio,

indicando il numero della postazione utilizzata. Questo allo scopo di poter risalire alle cause di eventuali inconvenienti o danneggiamenti e per comprovare l'effettivo utilizzo dell'aula.
4. L'ingresso degli allievi nei laboratori è consentito solo in presenza dell'insegnante.
5. Il docente accompagnatore è responsabile del corretto uso didattico di hardware e software.
6. Nei laboratori è vietato utilizzare CD personali o altri dispositivi se non dopo opportuno controllo con sistema di antivirus aggiornato.
7. All'uscita dal laboratorio sarà cura di chi lo ha utilizzato lasciare il locale in ordine e le macchine spente correttamente
8. In caso di malfunzionamento o guasto dei computer bisogna darne tempestiva segnalazione al responsabile del laboratorio.
9. L'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante.
Il Responsabile di laboratorio che verifichi un uso del laboratorio contrario a disposizioni di legge o del regolamento interno deve darne comunicazione per iscritto al Dirigente Scolastico.

Cap. 5 PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

5.1 PREVENZIONE

L'introduzione delle TIC nella didattica implica da parte degli insegnanti il dovere di imparare a riconoscere i rischi più comuni in cui i ragazzi possono imbattersi sul web, nonché quello di trasmettere agli stessi quegli strumenti di autotutela necessari ad un uso sicuro di Internet .

I rischi

I pericoli che gli alunni possono correre a scuola derivano da un uso scorretto dei dispositivi elettronici, in particolare di quelli personali, che vengono utilizzati furtivamente eludendo la sorveglianza degli insegnanti.
Tra i principali rischi in cui i ragazzi possono imbattersi figurano:

- possibile esposizione a contenuti inappropriati e non adatti alla loro età (razzismo, comportamenti alimentari scorretti, istigazione alla violenza …);
- violazione della privacy;
- dipendenza da Internet;
- pubblicità ingannevoli;
- *cyber-bullismo* (molestie o maltrattamenti da coetanei);
- videogiochi diseducativi;
- accesso ad informazioni scorrette;
- *virus* informatici in grado di infettare *computer* e cellulari;
- *sexting* (scambio di materiale a sfondo sessuale);
- *grooming* (adescamento *on line*).

Le azioni

Rispetto ai rischi sopra elencati l'I.C. Matteo Ricci intraprende le seguenti azioni di contrasto mirato:

- cogliere ogni opportunità per riflettere insieme agli alunni su tali rischi;
- costante monitoraggio delle relazioni interne onde individuare possibili situazioni di disagio ed attuazione tempestiva di un intervento educativo efficace;
- promozione continua di un clima positivo, di reciproca accettazione e rispetto;
- partecipazione a progetti e/o iniziative esterne selezionate e significative promosse da Enti e/o Associazioni di comprovata affidabilità;
- diffusione di un'informazione capillare rivolta al personale scolastico, agli studenti e alle famiglie, sui rischi che i minori possono correre sul web, attraverso la condivisione di materiali tratti dal sito di Generazioni Connesse;
- richiesta di autorizzazione esplicita da parte dei genitori all'utilizzo dei dati personali degli alunni (es. liberatoria per la pubblicazione di foto, immagini, video relativi al proprio/a figlio/a per la partecipazione a progetti didattici e altro);
- far rispettare il divieto di utilizzo di dispositivi digitali propri agli studenti in orario scolastico. Le dovute eccezioni (uso del cellulare per comunicazioni alunno-famiglia in occasione di uscite didattiche) andranno espressamente regolamentate e dovranno comunque avvenire sotto la supervisione diretta di un docente responsabile;
- dotare i dispositivi della scuola di filtri che impediscano l'accesso a siti web non adatti ai minori (black list).

5.2 RILEVAZIONE

Accorgersi di episodi di cyber bullismo non è sempre facile perché le prevaricazioni avvengono nei luoghi virtuali in cui gli adolescenti si ritrovano ed è necessario cogliere i segnali che i ragazzi ci lanciano quando si trovano in una situazione di disagio o di difficoltà. Per interpretare meglio questi segnali ed identificare il problema i docenti possono servirsi dei materiali di supporto forniti dal sito www.generazioniconnesse.it .

Che cosa segnalare

Le tipologie di comportamenti online da segnalare sono:

- Offese e insulti tramite messaggi di testo, e-mail, pubblicati su social network o tramite telefono (ad esempio telefonate mute);
- Diffusione di foto o video che ritraggono situazioni intime, violente o spiacevoli tramite il cellulare, siti web o social network;
- Esclusione dalla comunicazione on-line, dai gruppi;
- Furto, appropriazione, uso e rivelazione ad altri di informazioni personali come le credenziali d'accesso all'account e-mail, social network, ecc.

Come segnalare: quali strumenti e a chi.

Gli **studenti** che avranno necessità di segnalare situazioni di rischio, oltre che rivolgendosi direttamente ai docenti di cui si fidano, potranno farlo anche attraverso:

- le "**bully boxes**": cassette situate in alcuni punti della scuola in cui gli studenti anonimamente potranno segnalare le proprie preoccupazioni o esperienze, scrivendole e imbucandole;

- lo “**sportello d’ascolto**”: psicologhe che mettono la propria competenza al servizio dei ragazzi.

Laddove il **docente** colga possibili situazioni di disagio connesse ad uno o più di uno tra i rischi elencati nel paragrafo "Prevenzione", dovrà informare il docente responsabile della sicurezza on line attraverso la compilazione dell’apposita scheda di segnalazione. La scheda di segnalazione dovrà essere redatta dal docente sia sulla base di eventi osservati direttamente a scuola, sia in riferimento ad eventi particolari che gli sono stati confidati da un alunno o da un genitore. Sarà compito del responsabile della sicurezza on line contattare il dirigente scolastico per avviare l’iter idoneo.

I **genitori** che vengano a conoscenza di situazioni di rischio accadute durante l’orario di lezione o anche al di fuori di esso, ma di cui reputano sia importante metterne a conoscenza i docenti per aiutarli a gestire situazioni disfunzionali tra gli alunni di una classe, possono rivolgersi ai docenti stessi della classe o al referente della sicurezza on line attraverso apposito appuntamento in orario di ricevimento.

Ulteriore strumento di supporto è la **help line** telefonica di Telefono Azzurro **1.96.96** attiva 24 ore al giorno.
Questa linea di ascolto accoglie qualsiasi richiesta di ascolto e di aiuto da parte di bambini/e e ragazzi/e fino ai 18 anni o di adulti che intendono confrontarsi su situazioni di disagio/pericolo in cui si trova un minorenne. Il servizio di helpline è riservato, gratuito e sicuro, dedicato ai giovani o ai loro familiari che possono parlare al telefono con professionisti qualificati relativamente a dubbi, domande o problemi legati all'uso delle nuove tecnologie digitali e alla sicurezza online.
Le informazioni personali sono strettamente riservate e non vengono condivise con altri senza espressa autorizzazione, tranne nei casi previsti per legge, ovvero nel caso in cui il bambino/adolescente sia in una situazione di grave pericolo.

Inoltre, ci si potrà avvalere anche di un servizio **Hotline** che si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la rete. I due servizi messi a disposizione dal **Safer Internet Center** sono il**“Clicca e Segnala”**di **Telefono Azzurro e “STOP-IT” di Save the Children**. Una volta ricevuta la segnalazione, gli operatori procederanno a coinvolgere le autorità competenti in materia.

Come gestire le segnalazioni.

Le tappe da seguire quando si presenta un caso di cyber bullismo sono:
- fermare immediatamente l’abuso;
- dare sostegno alla vittima;
- lavorare sul gruppo classe affinché riconosca la gravità dell’accaduto e la propria partecipazione attraverso il silenzio o forme blande di coinvolgimento;
- dare supporto al bullo con un programma educativo che si focalizzi su due fronti: il coinvolgimento attivo del gruppo dei pari per sviluppare l’empatia e l’intervento dei docenti per gestire l’aggressività e la rabbia.

Il coinvolgimento dei coetanei è indispensabile per garantire l’efficacia dell’intervento ed è finalizzato a:
- creare un clima di solidarietà

- combattere l'indifferenza e la deresponsabilizzazione morale
- incoraggiare le vittime a chiedere aiuto
- sottrarre al cyberbullo potenziali proseliti.

5.3 GESTIONE DEI CASI

Definizione delle azioni da intraprendere a seconda della specifica del caso.

Innanzitutto se si ritiene che il materiale offensivo sia illegale la scuola ha il dovere di contattare la polizia postale. Nel caso in cui si trattasse di foto e video pedopornografici, il docente ha l'obbligo di confiscare il telefonino o eventuali altri dispositivi avendo cura di evitare di eseguire download, produrne copie, condividerne link o postarne il contenuto poiché ciò è reato per chiunque.

a) Casi di cyberbullismo:

Si definiscono bullismo tutte quelle situazioni caratterizzate da ***volontarie e ripetute aggressioni*** mirate a insultare, minacciare, diffamare e/o ferire una persona (o a volte un piccolo gruppo). Si tratta, pertanto, di una serie di comportamenti portati avanti ripetutamente nel tempo. Si parla di ***cyberbullismo*** quando queste forme di prevaricazione reiterate nel tempo si estendono anche alla vita online.
Tale specifica forma di bullismo ha caratteristiche peculiari:
1) è pervasivo: il bullo può raggiungere la sua vittima in qualsiasi momento e in qualunque luogo;
2) è un fenomeno persistente: il materiale messo online vi può rimanere per molto tempo;
3) spettatori e cyberbulli sono potenzialmente infiniti: le persone che possono assistere agli atti di cyberbullismo sono potenzialmente illimitate.

Occorre tenere presente che il cyberbullo non è mai del tutto consapevole della gravità dei suoi comportamenti se non viene aiutato ad esserne consapevole.
Qualora ci si trovi di fronte ad un caso di cyberbullismo si dovrà:

- informare i genitori degli alunni coinvolti;
- coinvolgere il referente di istituto dell'*e-safety* e gli operatori scolastici su quanto sta accadendo;
- coinvolgere la comunità scolastica in percorsi di prevenzione dei comportamenti a rischio online;
- tenere traccia di quanto successo e delle azioni intraprese, compilando un "diario di bordo" per consentire ulteriori indagini se necessarie.

b) Casi di sexting:

Qualora ci si trovi di fronte a un caso di sexting, cioè di invio e/o di ricezione e/o di condivisione di testi, video o immagini sessualmente espliciti via cellulare o tramite internet, si dovrà:

- coinvolgere la classe e confrontarsi con esperti, facendo appello, per esempio, allo sportello d'ascolto dell'istituto per capire come approfondire e affrontare il fenomeno;
- coinvolgere la comunità scolastica in percorsi di prevenzione dei comportamenti riconducibili al *sexting*;
- documentarsi opportunamente sulle norme giuridiche che regolano i comportamenti e le condotte sessuali in Italia;

- intraprendere con la classe attività mirate a riflettere sulla fiducia che ciascuno ripone negli altri e sul fenomeno del *sexting*, approfondendo casi e testimonianze.

c) Casi di adescamento online o *grooming*:

Le tecnologie digitali consentono ai giovani di ampliare la propria rete di amicizie in modo quasi smisurato: non di rado gli adolescenti "concedono" la loro amicizia non solo a persone che conoscono direttamente, ma anche ad "amici di amici". Questo li espone a rischi notevoli, come quello di dare accesso a sconosciuti al loro mondo online e quindi a informazioni personali.
L'adescamento online (*grooming*) consiste nel tentativo, da parte di un adulto, di avvicinare un/a bambino/a o adolescente per scopi sessuali, conquistandone la fiducia attraverso l'utilizzo della rete Internet (tramite chat, blog, forum e social networks, per esempio).In un primo tempo, l'adulto, spesso mentendo sulla propria identità e sulla propria età, mostra particolare interesse nei confronti del/la bambino/a o dell'adolescente, cercando di conquistarne la fiducia. Solo in un secondo tempo, cerca di entrare sempre più nell'intimità del bambino fino a introdurre argomenti intimi e attinenti alla sfera sessuale.
È bene che anche gli insegnanti aiutino i propri alunni a tutelarsi, scegliendo con cura chi frequentare online, per evitare che una condotta imprudente possa comportare ripercussioni non banali nella loro vita reale.
Una volta riconosciuti alcuni segni che possono rinviare a una situazione di adescamento online, quali un improvviso calo nel rendimento scolastico; un aumento del tempo trascorso dall'alunno online congiunto ad una particolare riservatezza al riguardo; allusioni da parte dell'alunno alla frequentazione di una persona più grande, o a regali ricevuti, ecc., è bene:

- approfondire la situazione coinvolgendo la classe e l'intera comunità scolastica;
- avviare dei percorsi di riflessione in classe sul concetto di fiducia;
- farsi affiancare da esperti, ricorrendo anche allo sportello d'ascolto per offrire ai minori, qualora lo desiderino, il supporto necessario.