MINISTERO DELL'ISTRUZIONE DELL'UNIVERSITA' E DELLA RICERCA
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
ISTITUTO COMPRENSIVO "Marino Centro"
00047 MARINO (RM) DISTRETTO 40 – RMIC8A100A
Via Olo Galbani – Tel e Fax 06/9385389
E-mail rmic8a100a@istruzione.it

E-SAFETY POLICY

Sommario

INTRODUZIONE

SCOPO DELLA POLICY

Le tecnologie digitali sono sempre più presenti nella vita quotidiana di tutti, così come negli ambienti scolastici, e bambini e adolescenti entrano in contatto con esse in età sempre più precoce. La presenza di tali tecnologie offre senza dubbio nuove opportunità a livello didattico, alle quali si accompagna la necessità di operare riflessioni e interventi volti ad un utilizzo che possa definirsi sicuro, consapevole e positivo in primo luogo da parte dei ragazzi, che delle tecnologie fanno un uso immediato e spesso poco consapevole proprio in virtù della grande diffusione delle tecnologie e dell'apparente semplicità che contraddistingue il loro utilizzo.

È pertanto necessario, da parte delle Istituzioni Scolastiche, avviare una politica di sicurezza della navigazione on line volta a un controllo dell'uso delle strumentazioni digitali e alla diffusione dell'adozione di buone pratiche di navigazione su Internet. Se bambini e giovanissimi mostrano un'innata predisposizione all'uso delle tecnologie, tuttavia, assai frequentemente a questa abilità non corrisponde un'adeguata e corretta capacità interpretativa della mole di informazioni alla quale essi sono di continuo sottoposti, in primo luogo attraverso i social network, i quali, se utilizzati in modo superficiale e inappropriato, possono trasformarsi in veicoli di cyber-bullismo.

Dall'esistenza di questo bisogno di promozione di un uso sicuro e positivo delle tecnologie scaturisce il presente documento, prodotto dall'IC Marino Centro, nell'ambito dell'adesione al progetto "Generazioni connesse", promosso dal Miur per offrire alle Istituzioni Scolastiche interessate un supporto effettivo nella definizione di misure di prevenzione, rilevazione e gestione delle problematiche derivanti da un uso non consapevole delle tecnologie digitali tra gli studenti, anche attraverso la formazione degli insegnanti e la sensibilizzazione dei genitori.

In sintesi, il documento intende costituire un primo step in questa direzione e fornire alcune linee guida rispetto alle azioni dell'Istituto in ordine a:

- utilizzo consapevole delle TIC[1] in ambiente scolastico e nella didattica prevenzione;
- gestione di situazioni problematiche connesse all'uso delle tecnologie digitali.

La futura implementazione e le eventuali modifiche migliorative che saranno apportate al documento assumono ancora maggiore rilevanza in considerazione del fatto che l'Istituto Comprensivo Marino Centro, anticipando la Legge n. 71 del 29 maggio 2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", si è dotata sin dal 2015 di una struttura organizzativa di prevenzione e contrasto ai fenomeni del Bullismo e del Cyberbullismo, attraverso il progetto Scuola Attiva, tuttora operante. Sempre in quell'anno è stato vincitore di un Bando della Regione Lazio per l'attivazione di un percorso di formazione in rete, presentato in partenariato con l'Ambulatorio sulla Dipendenza da Internet del Policlinico Gemelli, che ha consentito la formazione intensiva sul fenomeno per i docenti. Dal 2016 l'IC Marino Centro è iscritto al Progetto del MIUR "Generazioni connesse" e nel 2018 riceve l'attestato di "Scuola Virtuosa". Dal 2015 ad oggi l'IC è attivo con servizi di supporto alle problematiche emotive e affettive dei ragazzi, dei genitori e dei docenti

[1] TIC o ICT, tecnologie dell'informazione e della comunicazione

con percorsi specifici di formazione e prevenzione, attualmente gestiti dalla Cooperativa Magliana ’80.

Il documento potrà dunque, se necessario, essere modificato e aggiornato annualmente in funzione di eventuali nuove esigenze e, di conseguenza, di nuove azioni da porre in essere anche nell’ottica di una sua piena integrazione con obiettivi e contenuti degli altri documenti di Istituto, primo tra tutti il PTOF.

1. Le principali aree di rischio

Le principali aree di rischio per la nostra comunità scolastica possono essere riassunte come segue:

a. Contenuto

- L’esposizione a contenuti inappropriati
- Visita di siti web inappropriati
- Siti di odio
- Giochi violenti e non appropriati all’età
- Uso distorto della chat e delle videochat. Gestione dei gruppi.
- Uso distorto dei Social Network
- Dipendenza da internet e da videogame
- Validazione dei contenuti: come controllare l’autenticità e l’esattezza dei contenuti online
- Fake News

b. Contatto

- Cyberbullismo in tutte le forme
- Furto d’identità
- Grooming

c. Condotta

- Privacy, divulgazione di informazioni personali (dati, immagini, ecc)
- Reputazione online
- Salute e benessere. Quantità di tempo speso su Internet e videogame
- Sexting (invio e ricezione di immagini personali intime).
- Qualità delle chat e dei gruppi ad esse relazionate.
- Copyright relativo a musica e film
- Divulgazione delle Fake News

2. Ruoli e Responsabilità

Ruolo	Responsabilità
IL DIRIGENTE SCOLASTICO	• Responsabilità generale per i dati e la sicurezza degli stessi • Accertarsi che la scuola utilizzi un Internet Service filtrato approvato, conforme ai requisiti di legge vigenti • La responsabilità di assicurare che il personale riceva una formazione adeguata per svolgere i ruoli di sicurezza online e per la formazione di altri colleghi • Essere a conoscenza delle procedure da seguire in caso di infrazione della E-Safety Policy • Controllare e disporre aggiornamenti sulla E-Safety Policy • Ricevere relazioni di monitoraggio periodiche della sicurezza online da parte del responsabile • Gestire le segnalazioni ai Servizi Sociali • Monitorare l'utilizzo corretto di G-Suite

REFERENTE CONTRO IL BULLISMO E IL CYBERBULLISMO	• Coordinare le iniziative di prevenzione e di contrasto del cyberbullismo, anche avvalendosi della collaborazione delle Forze di polizia nonché delle associazioni e dei centri di aggregazione giovanile presenti sul Territorio (L. 71/2017, art. 4, c. 3) • Raccogliere e diffondere le buone pratiche educative, organizzative e azioni di monitoraggio. • Supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav). (Linee di orientamento) • Promuovere la consapevolezza e l'impegno per la salvaguardia online in tutta la comunità scolastica • Garantire che tutto il personale sia a conoscenza delle procedure che devono essere seguite in caso di incidente per la sicurezza online • Garantire che sia tenuto un registro di incidente di sicurezza online • Garantire che sia dedicata e costantemente aggiornata una bacheca informativa, in ogni Plesso della Scuola, dedicata agli alunni e ai genitori • Garantire la massima diffusione ai docenti, genitori e alunni, dei contenuti di prevenzione e contrasto ai fenomeni • Controllare che sia posto in ogni Plesso una cassetta per le segnalazioni e pubblicizzata la mail dedicata • Facilitare la formazione e la consulenza per tutto il personale • Coordinare interventi con le autorità locali e le agenzie competenti • Facilitare la creazione di Reti significative e funzionali con il territorio • Raccordarsi con il Dirigente Scolastico e il suo staff • Accogliere e supportare i genitori e gli alunni in difficoltà • Patrocinare gli interventi di formazione e prevenzione con le ASL e l'Ambulatorio contro le Dipendenze del Policlinico Gemelli di Roma. • Monitorare l'utilizzo corretto di G-Suite

RESPONSABILI DI PLESSO	• Monitorare la sicurezza online nel Proprio Plesso • Esaminare casi segnalati e coordinare gli interventi. • Promuovere la consapevolezza e l'impegno per la salvaguardia online • Assicurare che l'educazione alla sicurezza online sia incorporata in tutto il programma di studi • Garantire che tutto il personale del Plesso sia a conoscenza delle procedure che devono essere seguite in caso di incidente per la sicurezza online. (per i Responsabili di Plesso). • Garantire che sia tenuto un registro di Plesso per eventuali incidenti riguardanti la sicurezza online • Facilitare la formazione e la consulenza per il personale del Plesso • Coordinare gli interventi con lo staff, il Dirigente ed eventualmente le autorità locali e le agenzie competenti • Monitorare l'applicazione delle norme sulla condivisione dei dati personali • Monitorare e segnalare l'accesso a materiali illegali o inadeguati • Controllare, gestire e segnalare probabili azioni di cyberbullismo • Applicare ognuno nella propria sede di lavoro le disposizioni di legge previste e le azioni di prevenzione e contrasto decise dall'Istituto • Garantire che tutto il personale sia a conoscenza delle procedure che devono essere seguite in caso di incidente per la sicurezza online • Garantire che sia tenuto un registro di incidente di sicurezza online • Garantire che sia dedicata e costantemente aggiornata una bacheca informativa, nel proprio Plesso, dedicata agli alunni e ai genitori. • Garantire la massima diffusione ai docenti, genitori e alunni, dei contenuti di prevenzione e contrasto ai fenomeni • Esporre, in maniera visibile, una cassetta per le segnalazioni e pubblicizzata la mail dedicata • Facilitare la formazione e la consulenza per tutto il personale • Accogliere e consigliare i genitori e gli alunni in difficoltà • Monitorare l'utilizzo corretto di G-Suite nel proprio Plesso

L'ANIMATORE DIGITALE E IL TEAM	• Pubblicare la E-Safety Policy sul sito della scuola • Pubblicare le iniziative di Scuola Attiva sul sito della scuola • Assistenza ai docenti per il controllo alla corretta navigazione • Diffusione delle netiquette sull'uso responsabile di internet • Diffusione della conoscenza di materiali per uso didattico in CC, Creative Commons e software open source. • Verifica dell'aggiornamento costante dell'antivirus e eliminazione applicazioni non autorizzate • Promuovere la formazione per i docenti e i genitori sulle tematiche in oggetto. • Amministrare, gestire e monitorare l'utilizzo corretto di G-Suite
GLI INSEGNANTI	• Inserire tematiche legate alla sicurezza online in tutti gli aspetti del programma di studi e di altre attività scolastiche • Supervisionare e guidare gli alunni con cura quando sono impegnati in attività di apprendimento che coinvolgono la tecnologia online • Garantire che gli alunni siano pienamente consapevoli delle capacità di ricerca e dei problemi legali relativi ai contenuti elettronici come ad esempio le leggi sul copyright. • Segnalare prontamente al Referente contro il bullismo e cyberbullismo, eventuali casi di cui si è venuto a conoscenza o se ne sospetta l'esistenza. • Formarsi sulle tematiche del cyberbullismo e della dipendenza da internet. • Diventare un punto di riferimento per i propri alunni in quanto a prevenzione, supporto e informazione. • Utilizzo corretto di G-suite e monitoraggio dell'uso da parte dei propri alunni.

IL PERSONALE SCOLASTICO	• Comprendere e contribuire a promuovere politiche di e-sicurezza • Essere consapevoli dei problemi di sicurezza online connessi con l'uso di telefoni cellulari, fotocamere e dispositivi portatili • Monitorare l'uso di dispositivi tecnologici e attuare politiche scolastiche per quanto riguarda questi dispositivi • Segnalare qualsiasi abuso sospetto o problema ai Responsabili di Plesso • Usare comportamenti sicuri, responsabili e professionali nell'uso delle tecnologie • Garantire che le comunicazioni digitali con gli studenti siano solo a livello professionale e solo attraverso sistemi scolastici, non attraverso chat o mail personali. • Utilizzo corretto di G-Suite

GLI ALUNNI	• Leggere, comprendere ed accettare la E-Safety Policy • Conoscere e rispettare le leggi sulla privacy e sul copyright • Capire l'importanza di segnalare abusi, minacce, atti di cyberbullismo o accesso a materiali inappropriati • Sapere quali azioni intraprendere se loro, o qualcuno che conoscono, si sente preoccupato o vulnerabile riguardo le nuove tecnologie • Conoscere e rispettare la politica della scuola relativa all'uso dei telefoni cellulari, tablet, fotocamere digitali e dispositivi portatili • Conoscere e capire la politica della scuola sull'uso di immagini e sul cyberbullismo • Capire l'importanza di adottare buone pratiche di sicurezza online quando si usano le tecnologie digitali fuori dalla scuola • Assumersi la responsabilità di conoscere i benefici e i rischi di utilizzo di internet e di altre tecnologie in modo sicuro, sia a scuola che a casa • Utilizzo corretto di G-Suite

I 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 attraverso incontri con la Polizia postale 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. I genitori saranno incoraggiati a sostenere la scuola nel promuovere le buone pratiche di e-safety e a seguire le linee guida sull'uso appropriato di: o immagini digitali e video registrati in occasione di eventi scolastici, anche al di fuori delle aule; o accesso alle sezioni del sito dedicate ai genitori, con particolare riguardo al registro elettronico; o dispositivi personali dei loro figli nella scuola. • Monitorare l'utilizzo corretto di G-Suite del proprio figlio

3. Condivisione e comunicazione della Policy all'intera comunità scolastica.

Il presente documento sarà pubblicato sul sito web della scuola, nella sezione dedicata alle azioni di contrasto al Bullismo/Cyber-bullismo, ed integrato, come allegato, nel PTOF (Piano Triennale per l'Offerta Formativa). Ciò garantirà una completa condivisione da parte dell'intera comunità scolastica e potrà rendere il documento una base di partenza per azioni e iniziative, quali una discussione aperta sui contenuti e sulle pratiche indicate, sulle modalità per inserire le tematiche di interesse della Policy nel curricolo, nonché un confronto in merito alla necessità di apportarvi modifiche e miglioramenti.
L'E-Safety Policy d'Istituto si applica a tutti i membri della scuola, compreso il personale, gli studenti, i genitori, gli utenti della comunità che ne hanno accesso.

La Policy sarà comunicata al personale, agli alunni, alla comunità nei seguenti modi:

- Pubblicazione della E-Safety Policy sul sito della scuola
- Accordo di utilizzo accettabile, discusso con gli studenti e i genitori, all'inizio del primo anno,

tramite il Patto di Corresponsabilità, che sarà sottoscritto dalle famiglie e rilasciato alle stesse
- Accordo di utilizzo accettabile rilasciato al personale scolastico
- Diffusione dell'E-Safety Policy in sede di: Consiglio d'Istituto, GLHI, Collegio dei docenti

4. Strategie d'intervento di prevenzione

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 LAN e WI-FI secondo i normali canali di protezione presenti nei sistemi operativi e delle chiavi di accesso alla rete.

Si attrezza per evitare comportamenti che non rientrano nelle norme che il Collegio dei Docenti e il Consiglio d'Istituto delineano in proposito, come:

- Scaricare file video-musicali protetti da copyright
- Scaricare CODEC e Software di dubbia provenienza
- Visitare siti non necessari o consoni all'attività didattica
- Alterare i parametri di protezione dei computer in uso
- Utilizzare la rete per interessi privati e personali che esulano dalla didattica

La scuola, inoltre, si impegna a:

- Tutelare i dati personali (immagini e dati sensibili)
- Garantire la presenza di Bacheche informative e Cassette per le segnalazioni in tutti i Plessi
- Favorire la presenza del Referente contro il Bullismo e il Cyberbullismo nelle reti istituzionali locali.
- Garantire la partecipazione attiva di tutti i componenti della scuola (Dirigente Scolastico, DSGA, genitori, alunni, docenti, personale scolastico, personale di segreteria)
- Garantire la partecipazione e supervisione al progetto Scuola Attiva degli organismi interni della scuola (Consiglio d'Istituto, Collegio dei Docenti, Staff, ecc)
- Promuovere cicli di formazione continua rivolti a docenti, genitori, alunni e personale scolastico.

Disposizioni, comportamenti, procedure:

- Il sistema informatico è periodicamente controllato dai responsabili (Funzione Strumentale, Animatore Digitale e Team Digitale)
- La scuola può controllare periodicamente la cronologia di navigazioni, le applicazioni scaricate, i file temporanei e i siti visitati da ogni pc
- La scuola archivia i tracciati del traffico internet
- E' vietato installare e scaricare da internet software non autorizzati
- E' vietato comunicare la chiave di accesso ad Internet agli alunni, se non dietro autorizzazione del Dirigente Scolastico (eccezion fatta per gli alunni delle classi 2.0 e 3.0)
- Antivirus e antimalware devono regolarmente essere aggiornati e periodicamente i computer devono essere sottoposti a scansione

- L'utilizzo di CD e chiavi USB devono essere autorizzate dal docente e solo previa scansione antivirus.
- La scuola si riserva di limitare il numero di siti visitabili e le operazioni di download
- Agli alunni sarà somministrato ogni anno un questionario online, previa autorizzazione dei genitori, per sondare la conoscenza e la presenza dei fenomeni di cyberbullismo, dipendenza da internet e da videogame
- Divieto di uso del cellulare senza autorizzazione e solo per motivazioni didattiche.
- Permesso di utilizzo di apparati tecnologici (tablet, pc, ecc..) solo per fini didattici e previa autorizzazione del Consiglio di Classe o del singolo docente.
- I docenti e il personale scolastico sono obbligati a segnalare casi di sospetto bullismo, cyberbullismo e dipendenza da internet al Dirigente Scolastico e allo Staff di Scuola Attiva per le conseguenti verifiche
- E' fatto obbligo, nell'utilizzo di G-Suite, di rispettare rigorosamente il Regolamento d'Uso

5. Strategie di contrasto ai fenomeni

Il Dirigente Scolastico regola il comportamento degli studenti e autorizza i membri del personale di imporre sanzioni disciplinari per il comportamento inadeguato. Questo è pertinente a episodi di cyberbullismo, o altri tipi di incidenti che possono danneggiare la sicurezza online. I provvedimenti disciplinari nei confronti dell'alunno che ha commesso un'infrazione alla policy dovranno essere proporzionati all'età dello studente e alla gravità dell'infrazione commessa

La scuola, attraverso i singoli Consigli di Classe e Team, si occuperà di tali incidenti all'interno di questa Policy, delle politiche di comportamento e antibullismo associati, e nel quadro normativo del Regolamento di Disciplina dell'Istituto e dello "Statuto degli Studenti e delle Studentesse", DPR 24 giugno 1998, n. 249, e avrà il compito di informare i genitori di episodi di comportamento inappropriato di sicurezza online, che si svolgono all'interno della scuola.

Per episodi segnalati, ma accaduti in spazi e tempi extrascolastici, la scuola informerà e coinvolgerà in ogni caso i genitori.

Qualora tali infrazioni dovessero configurarsi come reato, se ne sarà data tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso. Infatti nel momento in cui un qualunque attore della comunità scolastica venga a conoscenza di un reato perseguibile d'ufficio, è fatto obbligo di denuncia (ex art. 331 del Codice di Procedura Penale).

6. Monitoraggio dell'implementazione della Policy e suo aggiornamento

La E-Safety Policy sarà riesaminata ogni due anni o quando si verificano cambiamenti significativi per quanto riguarda le tecnologie in uso all'interno della scuola e tutte le modifiche della Policy saranno discusse in dettaglio con tutti i membri del personale docente.

Nell'ambito della revisione della Policy, tutte le informazioni e le revisioni saranno memorizzate per eventuali controlli, sulla base del seguente documento

Nome	E-Safety Policy IC Marino Centro
Versione	2.0
Data revisione	25/06/2020
Autore	Prof. Luca Congedo, Referente contro il Bullismo e Cyberbullismo dell'IC Marino Centro
Approvato dal Dirigente	25/06/2020
Approvato dal Consiglio d'Istituto	27/06/2020
Approvato dal Collegio dei Docenti	25/06/2020
Prossima data di revisione	06/2022
Modifica	

Nell'ambito del monitoraggio dell'implementazione della E-Safety Policy si terranno in considerazione i dati annuali sulla base del seguente documento

ANNO	NUMERO DI SEGNALAZIONI	NUMERO DI INFRAZIONI	NUMERO DI SANZIONI DISCIPLINARI

7. FORMAZIONE E CURRICOLO

Il Piano Nazionale Scuola Digitale (PNSD) ha l'obiettivo di modificare gli ambienti di apprendimento per rendere l'offerta formativa di ogni istituto coerente con i cambiamenti della società della conoscenza e con le esigenze e gli stili cognitivi delle nuove generazioni. Il PNSD, con valenza pluriennale, è quindi un'opportunità per innovare la Scuola, adeguando non solo le strutture e le dotazioni tecnologiche a disposizione dei docenti e dell'organizzazione, ma soprattutto le metodologie didattiche e le strategie usate con gli alunni in classe.

Il D.M. 851 del 27 ottobre 2015, in attuazione dell'art. 1, comma 56 della legge 107/2015, ne ha previsto l'attuazione al fine di:

- Migliorare le competenze digitali degli studenti anche attraverso un uso consapevole delle stesse
- Implementare le dotazioni tecnologiche della scuola al fine di migliorare gli strumenti didattici e laboratoriali ivi presenti
- Favorire la formazione dei docenti sull'uso delle nuove tecnologie ai fini dell'innovazione didattica, in particolare nell'utilizzo di G-Suite
- Individuare un Animatore Digitale ed un team per l'innovazione digitale che supporti ed accompagni adeguatamente l'innovazione didattica, nonché l'attività dell'Animatore Digitale
- Partecipare a bandi nazionali ed europei per finanziare le suddette iniziative

a. *Curricolo sulle competenze digitali per gli studenti*

Nell'ambito del PNSD questa scuola si propone un programma di progressiva educazione alla sicurezza online come parte del curriculum scolastico. Si impegna a sviluppare una serie di competenze e comportamenti adeguati all'età degli alunni e ad esperienza, tra cui:

- Programmare attività e far partecipare gli alunni a laboratori specifici sul digitale e la sicurezza in rete
- Sviluppare una serie di strategie per valutare e verificare le informazioni prima di accettare l'esattezza
- Essere a conoscenza delle fonti delle notizie in rete e che l'autore di un post o un sito web/pagina può avere un particolare pregiudizio
- Sapere come restringere o affinare una ricerca
- Riconoscere un comportamento accettabile quando si utilizza un ambiente online, vale a dire, essere educato, non utilizzare comportamenti inappropriati, mantenere le informazioni personali private
- Conoscere e seguire la netiquette
- Capire come le fotografie possono essere manipolate e individuare contenuti web in grado di attrarre il tipo sbagliato di attenzione
- Comprendere l'esistenza e saper riconoscere i profili fake e le false identità degli interlocutori in chat e social network
- Capire il motivo per cui non dovrebbero inviare o condividere resoconti dettagliati delle loro vite personali e informazioni di contatto
- Capire il motivo per cui non devono pubblicare foto o video di altri senza permesso
- Comprendere la motivazione del divieto di utilizzo dei cellulari a scuola
- Comprendere l'importanza di non scaricare file, software coperti da copyright o di dubbia natura
- Conoscere e contrastare i fenomeni di bullismo e cyberbullismo in tutte le sue forme.
- Sapere come chiedere aiuto e segnalare atti di bullismo e cyberbullismo
- Utilizzare con attenzione Internet per garantire che si adatti alla loro età e supporti gli obiettivi di apprendimento per le aree curricolari specifiche
- Conoscere e saper utilizzare positivamente le potenzialità delle nuove tecnologie e del mondo digitale.
- Conoscere le risorse digitali nel complesso, non esclusivamente legate al lato applicativo.

b. *Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali*

Nell'ambito del PNSD questa scuola ha previsto:

- Individuazione e formazione di un Animatore Digitale che come docente accompagnerà il Dirigente Scolastico e il DSGA nell'attuazione degli obiettivi e delle innovazioni previste dal PNSD
- Formazione dei docenti all'utilizzo delle TIC, in particolare nell'utilizzo di G-Suite.
- Creazione spazio di assistenza in itinere tramite piattaforma Weschool.
- Si assicura che il personale sa come inviare o ricevere dati sensibili o personali e comprendere l'obbligo di crittografare i dati dove la sensibilità richiede protezione degli stessi
- Offre una formazione a disposizione del personale in materia di sicurezza online attraverso corsi di aggiornamento
- Fornisce informazioni a tutto il nuovo personale circa le indicazioni presenti sulla E-Safety Policy d'Istituto.

c. *Sensibilizzazione delle famiglie*

Questa scuola esegue un programma continuativo di consulenza, orientamento e formazione per i genitori, tra cui:

- Presentare ai genitori il Regolamento della Policy, al fine di garantire che i principi di comportamento sicuro online siano chiari
- Bacheche informative e dedicate in ogni Plesso
- Mail a disposizione per i genitori e gli alunni per informazioni, segnalazioni e supporto
- Offrire incontro di consulenza con lo staff di Scuola Attiva
- Sezione dedicata sul sito internet della scuola
- Fornire informazioni sui siti nazionali di sostegno per i genitori, quali il sito www.generazioniconnesse.it
- Sportello psicologico gratuito
- Corsi di formazione per i genitori sulle tematiche della corretta navigazione

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

a. *Email*

Questa scuola ha predisposto per tutto il personale e per tutti gli alunni una mail istituzionale @icmarinocentro.edu.it, fornito da G-Suite, che diventa l'unico canale autorizzato di invio comunicazioni tramite mail, eccezion fatta per la mail ufficiale rmic8a100a@istruzione.it
Questa scuola non pubblica indirizzi di posta elettronica personali degli alunni o del personale sul sito della scuola, eccezion fatta per mail istituzionali di area.

Ogni mail segnalata come non appropriata sarà vagliata dal Dirigente Scolastico
Ove si riscontrano presunte infrazioni di legge, queste mail saranno segnalate alle autorità competenti.
Mail di spam, di phishing, virus e malware allegati possono risultare particolarmente pericolose. Perciò si utilizzeranno una serie di tecnologie per proteggere utenti e sistemi nella scuola, tra cui Antivirus e antimalware.

b. *Sito web della scuola*

L'istituto dispone di un sito web e di un proprio dominio https://www.icmarinocentro.edu.it
L'istituto gestisce un proprio sito web nello spazio di proprietà. La gestione del sito della scuola e la rispondenza alle normative per quanto concerne i contenuti (accuratezza, appropriatezza, aggiornamento e accessibilità) e le tecniche di realizzazione e progettazione è a cura del webmaster (Funzione Strumentale ins. Paolo Aghemo).
La scuola detiene i diritti di autore dei documenti che si trovano sul proprio sito o di quei documenti per i quali è stato chiesto ed ottenuto il permesso dell'autore proprietario. Le informazioni pubblicate sul sito della scuola relativo alle persone da contattare rispetteranno le norme vigenti sulla privacy.

La scuola, in qualità di ente pubblico, pubblicherà sul proprio sito web i contenuti che saranno valutati come pertinenti alle finalità educative istituzionali, ponendo attenzione alla tutela della privacy degli studenti e del personale, secondo le disposizioni normative.

c. *Sicurezza Rete Lan*

L'istituto, nella sede centrale, dispone di un dominio su rete locale (rete segreteria) cui accedono i computer dell'amministrazione, tali postazioni sono su una rete locale isolata dal resto della rete d'Istituto (rete didattica). Una linea LAN è dedicata esclusivamente al computer del Dirigente Scolastico. Il collegamento di computer portatili o palmari personali alla rete d'Istituto deve essere autorizzato dal Dirigente Scolastico.

Tutte le sedi sono provviste di Rete LAN.
La rete interna è protetta da Firewall per quanto riguarda le connessioni con l'esterno. Le postazioni sono protette con sistemi antivirus e antimalware regolarmente aggiornati.

La memorizzazione dei documenti e delle impostazioni personali è garantita attraverso il meccanismo di profili mobili di Windows, che archivia centralmente sul server di dominio i dati, e li rende disponibili in tutte le postazioni legate alla didattica (laboratori, sale insegnanti, classi). Su questi dispositivi non è garantito alcun servizio di backup, pertanto si consiglia di fare copia su un supporto personale.

Per quanto concerne la rete amministrativa, lo storage è garantito da backup automatico su Cloud.

d. *Sicurezza della rete senza fili (Wireless – WIFI)*

L'Istituto, in tutti i suoi plessi, dispone di una rete con tecnologia senza fili. L'accesso alla rete wireless è regolamentato dalla chiave di accesso.

L'ottenimento della chiave d'accesso è riservato solo agli autorizzati.
Le regole di comportamento sono analoghe a quelle per la connessione alle reti cablate dell'Istituto.

L'Istituto dato il numero sempre più alto di cl@ssi 2.0 e 3.0 valuterà un sistema di Mobile Device Management con doppia funzionalità di controllo, a scuola attraverso un pannello di amministrazione dei docenti, a casa con le scelte dei genitori e/o tutori (scelta di app e di orari di utilizzo)

9. Strumentazione personale

a. *Per gli studenti: gestione degli strumenti personali*

Come da Regolamento d'Istituto agli studenti è vietato l'utilizzo del cellulare all'interno della scuola. Per quanto concerne l'utilizzo del tablet o del pc, questi possono essere utilizzati solo in presenza del docente e per ragioni prettamente didattiche.

b. *Per i docenti e per il personale della scuola: gestione degli strumenti personali*

I docenti e il personale della scuola possono utilizzare smartphone e tablet esclusivamente a fini didattici e istituzionali (Compilazione del Registro Elettronico, ricerche didattiche, consultazione siti istituzionali, ecc.).

10. Prevenzione, rilevazione e gestione dei casi

a. *Prevenzione*

Principi generali:

b. Internet favorisce la libertà d'espressione e, quando si entra a far parte di una community o di un servizio dove interagiscono più utenti, vanno considerati abusi meritevoli di segnalazione solo i contenuti palesemente impropri o illeciti e non tutti quei contenuti con cui semplicemente non si è d'accordo o non piacciono.

c. Quando si inizia a navigare tra i servizi dei Social Network e le applicazioni web come Youtube, Instagram, Facebook, Netlog, ecc. bisogna informarsi subito su quali sono i diritti e i doveri dell'utente, leggendo il regolamento, tenendosi aggiornati, esplorando i siti informativi e istituzionali che affrontano queste tematiche.
d. Se si condividono informazioni personali, bisogna farlo scegliendo con cura che cosa rendere pubblico e cosa rendere privato. È indispensabile scegliere con attenzione le amicizie con cui accrescere la propria rete e i gruppi a cui aderire, proteggendo la propria identità digitale con password complesse e usando una domanda di recupero password della risposta non banale
e. 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 video girati di nascosto e dove sono presenti persone filmate senza il loro consenso.
f. 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.
g. 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. Prima di trasformare un incidente o una "bravata" in una denuncia alle autorità competenti avvalersi della modalità di segnalazione che non obbliga le parti in causa a conseguenze penali e giudiziarie che possono durare anni.

Scuola e Famiglia possono essere determinanti nella diffusione di un atteggiamento mentale e culturale che consideri la diversità come una ricchezza e che educhi all'accettazione, alla consapevolezza dell'altro, al senso di comunità e della responsabilità collettiva. Occorre, pertanto, rafforzare e valorizzare il Patto Educativo di Corresponsabilità previsto dallo Statuto delle Studentesse e degli Studenti della Scuola Secondaria: la scuola è chiamata ad adottare misure atte a prevenire e contrastare ogni forma di violenza e di prevaricazione; la famiglia è chiamata a collaborare, non solo educando i propri figli, ma anche vigilando sui loro comportamenti.
Per definire una strategia ottimale di prevenzione e di contrasto, le esperienze acquisite e le conoscenze prodotte vanno contestualizzate alla luce dei cambiamenti, che hanno profondamente modificato la società, sul piano etico, sociale e culturale e ciò comporta una valutazione ponderata delle procedure adottate per riadattarle in ragione di nuove variabili, assicurandone in tal modo l'efficacia.

La forma online del bullismo ha però alcune caratteristiche peculiari che lo rendono pericoloso perché:

1. *Il cyberbullismo è pervasivo:* il cyberbullo può raggiungere la sua vittima in qualsiasi momento e in qualsiasi luogo. Il possesso generalizzato di smartphone, anche nella scuola Primaria, sempre accessi e connessi ad internet permette al cyberbullo di aggredire la sua vittima ogni volta che lo desidera.
2. *È un fenomeno persistente:* il materiale diffamatorio pubblicato su internet può rimanere disponibile online per molto tempo, se non per sempre.

3. *Spettatori e cyberbulli sono potenzialmente infiniti* le persone che possono assistere ad episodi di cyberbullismo sono potenzialmente illimitate e molti possono essere cyberbulli, anche solo condividendo o promuovendo l'episodio di cyberbullismo, che finisce per replicarsi (ad esempio sulle bacheche dei profili che i ragazzi hanno sui Social Network) in modo incontrollabile.

b. *Azioni*

La scuola si impegna a:

- Riconoscere il Dirigente Scolastico come titolare del trattamento di dati personali secondo la GDPR art. 28 e al D. Lgs. 10 agosto 2018, n. 101
- Riconoscere come tutori della sicurezza online il DSGA, l'Animatore Digitale e il Team Digitale;
- Rendere aggiornata e attiva la piattaforma G-Suite

I docenti si impegnano a:

- Accompagnare gli alunni nella navigazione in Rete, coinvolgendoli nell'esplorazione delle opportunità e dei rischi, con attività calendarizzate dall'inizio dell'anno.
- Sostenere gli alunni nel corretto uso della piattaforma di G-Suite
- Approfondire, con attività mirate in classe, la conoscenza del fenomeno del bullismo e del cyberbullismo
- Creare degli spazi in cui gli alunni si possano confrontare su questo tema, utilizzando come spunti di riflessione: film, canzoni, incontri con esperti, letture mirate, lavori di gruppo sulle tematiche.
- Riferirsi al Referente contro il Bullismo e il Cyberbullismo per le tematiche in oggetto
- Rivolgersi alla helpline di generazioni connesse www.generazioniconnesse.it

I genitori si impegnano a:

- Firmare il Patto Educativo di Corresponsabilità redatto dalla scuola
- Prendere visione della E-Safety Policy messa a disposizione di docenti, genitori ed alunni sul sito della scuola https://www.icmarinocentro.edu.it
- Seguire le azioni promosse dalla scuola per un uso corretto della rete
- Frequentare corsi di formazione/convegni che la scuola organizzerà per la diffusione di informazioni legate ad un uso corretto della tecnologia digitale.
- Usare i gruppi dei genitori sulle webchat (Whatsapp, ecc) in maniera responsabile e senza divulgare notizie, non verificate, che potrebbero generare inutili allarmismi o sfociare in vere e proprie calunnie.
- Sostenere i propri figli nell'utilizzo corretto di G-Suite

Gli alunni si impegnano a:

- Prendere visone del Patto Educativo di Corresponsabilità che i genitori hanno firmato con la scuola
- Prendere visione della E-Safety Policy pubblicata sul sito web della scuola;
- Rispettare le regole per un uso corretto delle tecnologie

- Utilizzare correttamente la piattaforma G-Suite, seguendo scrupolosamente il Regolamento d'Uso e le indicazioni fornite dal proprio insegnante.
- Denunciare qualsiasi caso di abuso online
- Prendere parte a qualsiasi evento che la scuola organizza in materia di sicurezza online

Rilevazione e gestione dei casi

Intervenire in situazione di cyberbullismo non è mai semplice: spesso si pensa di non sapere esattamente cosa fare e si ha timore di essere inadeguati. Per tale motivo la scuola ha attivato il progetto Scuola Attiva che ha al suo interno docenti formati nel Corso di Formazione "Prevenzione e contrasto al bullismo, cyberbullismo e dipendenza da internet" con gli esperti dell'Ambulatorio contro le Dipendenze del Policlinico Gemelli di Roma.

La scuola si impegna ad individuare due strumenti che potranno agevolare l'intera comunità scolastica:

1. Nel decidere come intervenire
2. Nel tenere traccia di ciò che è avvenuto rispetto ai comportamenti degli alunni online e di come è stato gestito il problema.

L'obiettivo a lungo termine, che come comunità scolastica ci diamo, è quello di creare una memoria condivisa non solo di ciò che accade nella scuola rispetto al web, ma anche di strutturare una fonte esemplificativa che possa orientare sempre più e sempre meglio le azioni di contrasto ad episodi che, nel tempo, potrebbero ripetersi.

Per una efficace gestione dei casi la scuola si riserva di utilizzare lo schema messo a disposizione sul sito www.generazioniconnesse.it con l'unica modifica consistente nell'informare sempre e costantemente i genitori degli eventi emersi. (Allegato 1)

Per poter tenere traccia di ciò che è avvenuto rispetto ai comportamenti degli alunni online e di come è stato gestito il problema, la scuola si riserva di utilizzare il "Diario di Bordo" messo a disposizione sul sito www.generazioniconnesse.it (Allegato 2).

La Scuola si impegna inoltre ad organizzare le seguenti attività di prevenzione al fenomeno:

- Organizzazione di Corsi di formazione per docenti, genitori, personale scolastico
- Monitoraggio sul tema del cyberbullismo attraverso il questionario https://goo.gl/forms/5M5iFiqOhQAsv7Ur1
- Partecipazione da parte di docenti, studenti e genitori a convegni e seminari sul tema del bullismo e del cyberbullismo
- Interventi di consulenza e supporto – su richiesta da parte della scuola – relativamente a casi di cyberbullismo
- Supporto psicologico ad alunni, genitori e docenti
- Laboratori sulle emozioni in tutte le classi (dalla scuola dell'infanzia alla scuola secondaria di I Grado

Annessi

1. Procedure operative per la gestione delle infrazioni alla Policy (allegato n. 3)
2. Procedure operative per la rilevazione, il monitoraggio e la gestione delle segnalazioni (Allegato n.1, n.2)

IL DIRIGENTE SCOLASTICO
Prof. Giuseppe Di Vico

DI VICO
GIUSEPPE
14.07.2020
14:23:17 UTC

REFERENTE CONTRO IL BULLISMO E IL CYBERBULLISMO
Prof. Luca Congedo

FUNZIONE STRUMENTALE AREA 6 E ANIMATORE DIGITALE
Ins. Paolo Aghemo
Paolo Aghemo