ISTITUTO COMPRENSIVO STATALE di VIA PALMIERI
Via Nicola Palmieri, 24/26 – 20141 MILANO – Tel. 02/884.44286Fax 02/884.66940
SCUOLA DELL'INFANZIA *"A. CASSONI"* - SCUOLE PRIMARIE *"C. BATTISTI"-"C. PERONE"*
SCUOLA SECONDARIA DI PRIMO GRADO *"S. PERTINI" ad Indirizzo Musicale*
Codice Meccanografico: MIIC8FV006– Codice Fiscale n. 80123850150
web: www.primariabattisti.it e-mail: MIIC8FV006@istruzione.it – MIIC8FV006@pec.istruzione.it

E-Safety Policy
a.s 2017/18

INDICE
E-Safety Policy

1. INTRODUZIONE

La nostra Scuola intende incrementare l'uso delle tecnologie informatiche nella didattica e nell'organizzazione generale della scuola affinché Internet diventi lo strumento sia per svolgere esperienze formative, sia per condurre in modo più efficiente le funzioni amministrative.

Internet è un'inestimabile risorsa per l'educazione e l'informazione, offre infinite opportunità per fare ricerca, comunicare, documentare il proprio lavoro, pubblicare elaborati e mettere in comune esperienze. Da un punto di vista amministrativo, grazie all'implementazione del sito internet della scuola, all'introduzione del registro elettronico e all'utilizzo della piattaforma web AXIOS Italia, a cui possono accedere Dirigente, docenti e dal prossimo anno scolastico genitori, alunni e personale amministrativo,diventerà più semplice gestire il sistema-scuola e aprire la stessa all'utenza con una comunicazione più tempestiva, chiara e trasparente.

Allo stesso tempo, l'uso sempre più pervasivo di piattaforme in rete e dispositivi portatili ha esposto gli utenti e in particolare i minori, i soggetti con divario digitale o con limitate competenze informatiche a nuovi rischi, tanto più rilevanti quanto meno è diffusa una cultura relativa ai modi legittimi di usare la rete e alla consapevolezza delle funzioni rese possibili.

E-Safety Policy e il progetto "Generazioni connesse"

La nostra Scuola ha deciso di sviluppare e attuare il progetto "Generazioni Connesse" (www.generazioniconnesse.it) attraverso la realizzazione di tre linee di intervento:

1. l'elaborazione di linee guida per una e-Safety Policy d'Istituto, cioè di un proprio codice di condotta nella prevenzione e gestione dei casi di cyberbullismo e di un regolamento di sicurezza informatica che ha preso come riferimento i principi proposti dal MIUR nel documento che riassume "La posizione italiana sui principi fondamentali di Internet";

2. la cittadinanza digitale con la promozione nei confronti degli alunni della competenza digitale e della cultura del rispetto di regole comuni nell'uso dei servizi telematici e lo sviluppo di regole di buon comportamento (Netiquette) riferite specialmente ai Social Network e della conoscenza delle condizioni del loro utilizzo;

3. la procedura per la gestione delle problematiche e un insieme di attività per la prevenzione dei rischi articolate in interventi nelle classi dei Peer-Z (allievi della scuola formati come peer educator),interventi della Polizia di Stato e Postale, formazione docenti e genitori, Progetti didattici di prevenzione, interventi di formazione rivolti agli alunni da parte del responsabile Cyberbullismo d'istituto, incontri con esperti del settore, ad esempio il 15 maggio 2018 presso la nostra scuola si è tenuto un incontro di formazione con le classi terze condotto dal Dottor Paolo Picchio della Fondazione dedicata a Carolina Picchio, adolescente suicidatasi nel 2013 dopo che venne diffuso in Rete un video a sfondo sessuale che aveva lei come protagonista.

PRINCIPI GENERALI

Quali principi generali cui attenersi in termini di etica e di buon uso dei servizi in rete, la nostra Scuola ha deciso di prendere come riferimento i principi proposti dal MIUR nel documento "La posizione italiana sui principi fondamentali di Internet" in cui i principi fondanti della rete sono suddivisi in cinque sezioni che identificano gli ambiti a cui tali principi afferiscono:

Principi generali: internet bene comune, internet strumento cruciale per lo sviluppo e l'esercizio dei diritti umani, neutralità della rete e architettura aperta, benefici della tecnologia e della rete, modello decisionale trasparente con il coinvolgimento di tutti i portatori di interesse (*stakeholder*);

A. Cittadinanza in rete: accesso all'infrastruttura indipendentemente dal luogo di residenza, punti di accesso ad internet, accesso e riutilizzo dei dati del settore pubblico, accessibilità come strumento di inclusione, diritti umani e libertà fondamentali in rete e per mezzo della rete, auto-organizzazione e autonomia degli individui in rete;
B. Consumatori e utenti della rete: competenze digitali, identità digitale, riservatezza, accesso, archiviazione e cancellazione dei dati personali;
C. Produzione e circolazione dei contenuti: condivisione dei contenuti e della conoscenza in rete, proprietà intellettuale in ambiente digitale;
D. Sicurezza in rete: infrastrutture di interesse nazionale, sicurezza in rete, internet, comunicazione di crisi e operazioni di soccorso, protezione dei soggetti deboli.

SCOPO DELLA POLICY

L'intento del nostro Istituto è quello di promuovere l'uso da parte degli alunni delle tecnologie digitali e di Internet in modo responsabile, di far acquisire competenze e corrette norme comportamentali, di prevenire e gestire problematiche che derivano da un utilizzo pericoloso o dannoso delle tecnologie digitali.

I nostri allievi dimostrano predisposizione all'uso delle tecnologie, tuttavia, troppo spesso,a questa abilità si oppone una incapacità, dovuta alla giovane età, di non interpretare bene tutte le informazioni a cui, incessantemente, sono sottoposti, soprattutto attraverso l'uso dei social network. Pertanto la scuola attua parallelamente attività di prevenzione, controllo e formazione di docenti, allievi e famiglie. L'uso delle nuove tecnologie, se non adeguatamente usati, può trasformarsi in una trappola attraverso cui i giovani possono diventare vittime o carnefici di cyberbullismo.

Dunque, la policy di e-safety nasce dalla rilevazione di questo bisogno ed è volto a definire:

- norme comportamentali e procedure per l'utilizzo delle tecnologie nell'ambito dell'Istituto;
- misure per la prevenzione e per la rilevazione e gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali.

Il Dirigente Scolastico, i docenti, in particolare il Referente per il Cyberbullismo, il docente della Funzione Strumentale Informatica e l'Animatore Digitale hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di indicare regole di condotta chiare per unuso critico e consapevole di internet anche a casa, per prevenire il verificarsi di situazioni pericolose.

Per l'elaborazione del presente documento ci si è avvalsi del materiale bibliografico, reperibile in rete e messo a disposizione da Generazioni Connesse.

RUOLI E RESPONSABILITÀ

Nell'ambito di questa policy sono individuati i seguenti ruoli e le principali responsabilità correlate:

1. i genitori devono contribuire, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete; incoraggiare l'impiego delle TIC da parte degli alunni nello svolgimento dei compiti a casa, controllando che tale impiego avvenga nel rispetto delle norme di sicurezza; agire in modo concorde con la scuola perla prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite;

2. il Dirigente scolastico deve garantire la sicurezza (tra cui la sicurezza online) dei membri della comunità scolastica, offrire a tutti gli insegnanti una formazione adeguata in merito a un utilizzo positivo e responsabile delle TIC, seguire le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola;

3.l'animatore digitale, il responsabile dell'area informatica, il referente bullismo/cyberbullismo collaboratori del dirigente, cercano di stimolare la formazione interna all'istituto negli ambiti di sviluppo della "scuola digitale" e fornire consulenza e informazioni al personale in relazione ai rischi online e alle misure di prevenzione e gestione degli stessi, monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola,nonchè proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola, assicurare che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate e curare la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti;

4.**il *Direttore dei servizi generali e amministrativi*** deve assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni; prevedere interventi di personale tecnico di assistenza per la soluzione di problematiche relative alla rete e all'uso del digitale segnalate dai docenti; garantire il funzionamento dei diversi canali di comunicazione della scuola (sportello, circolari,sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet;

5.i docentidevono informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento; garantire che le modalità di utilizzo corretto e sicuro delle TIC e di internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi; garantire che gli alunni capiscano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet;garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali; assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente; controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche,ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito); nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti

controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei.
Infine non va sottovalutato il ruolo degli ***studenti*** come primi attori del percorso di acquisizione della capacità di positiva gestione delle proprie competenze digitali: in tale ottica si rende indispensabile coinvolgere anche i più giovani, non solo quali destinatari,ma anche interlocutori attivi e propositivi di tutte le azioni e gli interventi volti alla piena attuazione della Policy.
In particolare, il ruolo degli alunni include i seguenti compiti:

- essere responsabili, in relazione al proprio grado di maturità e di apprendimento, per l'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;
- avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali ma anche della necessità di evitare il plagio e rispettare i diritti d'autore;
- comprendere l'importanza di adottare buone pratiche di sicurezza online quando si utilizzano le tecnologie digitali per non correre rischi;
- adottare condotte rispettose degli altri anche quando si comunica in rete;
- esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori.

CONDIVISIONE E COMUNICAZIONE DELLA POLICYALL'INTERA COMUNITÀ SCOLASTICA

1. Condivisione e comunicazione della Policy agli alunni:

- all'inizio dell'anno, in occasione dell'illustrazione del regolamento d'istituto agli alunni da parte dei docenti, verrà presentata la policy, insieme ai regolamenti correlati;
- nel corso dell'anno saranno dedicate da ciascun docente alcune lezioni sulle buone pratiche per un utilizzo sicuro del digitale, con specifico riferimento ai rischi della rete e alla lotta al cyberbullismo.

2. Condivisione e comunicazione della Policy al personale:

- Le norme adottate dalla scuola in materia di sicurezza nell'utilizzo del digitale saranno discusse negli organi collegiali (collegio docenti, riunioni di dipartimento,consigli di classe) e rese note all'intera comunità scolastica tramite pubblicazione del presente documento sul sito web della scuola;
- Il personale della scuola riceverà un'adeguata informazione/formazione sull'uso sicuro e responsabile di internet, attraverso materiali resi disponibili anche sul sito web della scuola.

3. Condivisione e comunicazione della Policy ai genitori:

- le famiglie saranno informate in merito alla linea di condotta adottata dalla scuola per un uso sicuro e responsabile delle tecnologie digitali e di internet attraverso la condivisione del presente documento e di materiali informativi specifici sul sito web della scuola;
- al fine di sensibilizzare le famiglie sui temi dell'uso delle TIC saranno organizzati dalla scuola incontri informativi, durante i quali si farà riferimento alla presente policy.

GESTIONE DELLE INFRAZIONI ALLA POLICY

Tutte le infrazioni alla presente Policy andranno tempestivamente segnalate al Dirigente Scolastico, che avrà cura di convocare le parti interessate onde valutare le possibili azioni da intraprendere.

1. Infrazioni degli alunni

È bene che i docenti introducano attività laboratori ali miranti a sviluppare nei loro alunni una sempre maggiore consapevolezza dei rischi legati a un uso imprudente e improprio del web e che forniscano loro, ogni qualvolta avvenga un'infrazione alle regole stabilite, gli strumenti per affrontare le conseguenze dei loro errori.

I provvedimenti disciplinari da adottare da parte del consiglio di classe nei confronti dell'alunno che ha commesso un'infrazione alla policy (in proporzione sia all'età dello studente sia alla gravità dell'infrazione commessa) saranno i seguenti:

- richiamo verbale;
- sanzioni estemporanee commisurate alla gravità della violazione commessa (assegnazione di attività aggiunti veda svolgere a casa su temi di Cittadinanza e Costituzione; divieto temporaneo di prendere parte alla ricreazione e simili);
- nota informative sul diario ai genitori;
- convocazione dei genitori per un colloquio con l'insegnante;
- convocazione dei genitori per un colloquio con il Dirigente scolastico.

2. Infrazioni del personale scolastico

Le infrazioni alla policy da parte del personale scolastico possono riguardare sia la mancata osservanza delle regole qui descritte sulla gestione della strumentazione, sia la mancata sorveglianza e pronto intervento nel caso di infrazione da parte degli alunni.

3. Infrazioni dei genitori

Compito precipuo dei genitori è supportare gli insegnanti e il personale scolastico nel riconoscimento e nella costruzione di azioni di contrasto efficacia i principali rischi rappresentati dalla navigazione in internet di utenti molto giovani e spesso poco accorti.

Nel caso di infrazione si prevedono interventi, rapportati alla sua gravità, che vanno dalla semplice comunicazione del problema, alla convocazione da parte dell'insegnante di classe o del Dirigente Scolastico.

2. FORMAZIONE E CURRICOLO

Per competenze digitali si intendono competenze che abilitano allo studio, e un domani al lavoro, in maniera aumentata, potenziata, sfruttando le tecnologie per i propri obiettivi, le proprie aspirazioni, i propri interessi personali. Al fine di promuovere la condivisione di buone pratiche per un uso consapevole delle risorse digitali, prevenendo e contrastando "ogni forma di discriminazione e del bullismo, anche informatico"come previsto dalla normativa vigente, 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.

CURRICOLO SULLE COMPETENZE DIGITALI PER GLI STUDENTI

La Raccomandazione del Parlamento Europeo e del Consiglio del 18 dicembre 2006 relativa alle competenze chiave per l'apprendimento permanente (2006/962/CE), individua la competenza digitale, ovvero il "saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione (TSI) per il lavoro, il tempo libero e la comunicazione." Su queste indicazioni l'Istituto ha attivato e attiverà un percorso sull'uso consapevole delle tecnologie con i seguenti obiettivi:

- promuovere un uso consapevole delle nuove tecnologie;
- sensibilizzare e attivare gli studenti sui rischi e i pericoli derivanti da un uso non corretto dei social network;
- favorire lo sviluppo di una cittadinanza attiva e responsabile;
- educare e sensibilizzare i minori ai rischi associati all'utilizzo di piattaforme di condivisione;
- conoscere e acquisire consapevolezza su natura, ruolo e opportunità delle TSI nel quotidiano;
- distinguere il reale dal virtuale, pur riconoscendone le correlazioni;
- sviluppare le abilità di base nelle TSI (uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni;
- acquisire consapevolezza su come le TSI possono coadiuvare la creatività e l'innovazione;
- riflettere sulle problematiche legate alla validità e all'affidabilità delle informazioni disponibili.

In virtù della valenza trasversale delle competenze digitali, la loro acquisizione verrà promossa attraverso percorsi didattici disciplinari e/o interdisciplinari inerenti diverse aree, coerentemente con gli obiettivi individuati nel curricolo di Istituto.

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

La Scuola ha partecipato con successo ai Fondi Strutturali Europei - Programma Operativo Nazionale "Per la scuola – Competenze e ambienti per l'apprendimento" 2014-2020, tali fondi permetteranno il miglioramento della connessione wi-fi e dell'aula 2.0.

La Scuola sta potenziando le aule di informatica e vorrebbe ampliare la dotazione di LIM.

È auspicabile che le azioni realizzate quest'anno inneschino un circolo virtuoso che stimoli sempre più docenti a utilizzare e integrare le TIC nella didattica.

Sicuramente saranno pianificate occasioni di formazione per apprendere l'utilizzo dell'aula 2.0e capirne le potenzialità e, probabilmente, saranno cercate risorse per partecipare a corsi di formazione sulle metodologie innovative e sull'integrazione delle TIC nella didattica. Nel prossimo anno scolastico, la Scuola metterà a diposizione dei software didattici con relativa formazione per il loro efficace utilizzo come richiesto dal gruppo docente che ha partecipato al Progetto

"generazioniconnesse".
La Scuola promuoverà inoltre la creazione dell'account sulla Piattaforma del sito "generazioniconnesse.it" per tutti i docenti, ambiente ricco di materiale didattico per supportare il corpo docente nelle creazione di Unità di Apprendimento mirate allo sviluppo delle competenze digitali degli allievi.

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

La partecipazione agli incontri organizzati all'avvio del progetto "Generazioni connesse"per alunni, genitori e docenti ha suscitato interesse, e vista la necessità di implementare la e-Safety Policy con il contributo di tutte le componenti, la Scuola prevede di organizzare per l'anno prossimo occasioni di confronto fra docenti sulle strategie più opportune da adottare come promozione dell'utilizzo consapevole e sicuro di Internet e delle TIC e come misure di prevenzione primaria al cyberbullismo,analizzando il fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica e promuovendo la partecipazione del corpo docente ai corsi di formazione sull'utilizzo dell'integrazione delle TIC nella didattica.
La Scuola promuoverà inoltre la creazione dell'account sulla Piattaforma del sito "generazioniconnesse.it" per tutti i docenti, dove potranno migliorare la loro formazione attraverso la proposta di vari corsi in cui ci si potrà iscrivere gratuitamente.
Si prevede di organizzare incontri con esperti e dei laboratori/eventi destinati a docenti, studenti e genitori per sensibilizzare l'intera comunità scolastica sui rischi della navigazione non controllata e su un corretto uso delle tecnologie digitali.

SENSIBILIZZAZIONE DELLE FAMIGLIE

Un incontro rivolto alle famiglie è stato effettuato in data 13 marzo 2018 con l'intervento degli operatori del progetto "Generazioni connesse", un altro a consuntivo sarà organizzato nel mese di maggio 2018: sarà rivolto a tutti i rappresentanti delle classi prime e seconde e ai rappresentanti per la componente genitori nel Consiglio d'Istituto della sede ed avrà la funzione di rendicontare le attività svolte durante l'anno scolastico per sensibilizzare gli alunni e di condividere le linee guida per la e-Safety Policy da implementare nel prossimo anno scolastico con la collaborazione dei genitori.
La scuola darà 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 non consapevole e critico del digitale.
Allo scopo di mantenere viva l'attenzione delle famiglie sull'uso responsabile e sicuro delle nuove tecnologie, l'Istituto promuove opportunità di incontro e formazione per le famiglie sui temi oggetto della Policy, offerte dal territorio, selezionando iniziative significative promosse da Enti e/Associazioni di comprovata affidabilità.

3.GESTIONEDELL'INFRASTRUTTURA,DELLASTRUMENTAZIONEITCDELLA SCUOLA

La scuola metterà in atto tutte le azioni necessarie per garantire agli studenti le ricerchein rete, adottando tutti i dovuti sistemi di sicurezza per diminuire le possibilità di rischio durante la navigazione.
Resta fermo che non è possibile garantire una navigazione totalmente priva di rischi e che la Scuola e gli insegnanti non possono assumersi le responsabilità conseguenti all'accesso accidentale e/o improprio a siti illeciti.

Leggi di riferimento

- Legge 29 Maggio 2017 n. 71 – Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo
- legge regionale Bullismo e Cyberbullismo
- Linee di orientamento per la prevenzione e il contrasto del cyberbullismo 2015
- Linee di orientamento per la prevenzione e il contrasto del cyberbullismo 2017

ACCESSO AD INTERNET: FILTRI, ANTIVIRUS E SULLA NAVIGAZIONE

Linee guida di buona condotta dell'utente

- Rispettare la legislazione vigente;
- Tutelare la propria privacy, quella degli altri utenti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni elettroniche cui hai accesso;
- Rispettare la cosiddetta netiquette (regole condivise che disciplinano il rapportarsi fra utenti della rete, siti, forum, mail e di qualsiasi altro tipo di comunicazione).

Le regole

- Rispettare le persone diverse per nazionalità, cultura, religione,sesso;
- Non rivelare dettagli o informazioni personali o di altre persone (indirizzi, numeri di telefono);
- Non dare indirizzo e numero di telefono a persone incontrate sul web;
- Non prendere appuntamenti con le persone conosciute tramite web;
- Non inviare fotografie proprie o di altre persone;
- Riferire sempre a insegnanti e genitori se si incontrano in Internet immagini o scritti che infastidiscono;
- Se qualcuno non rispetta queste regole è necessario parlarne con genitori ed insegnanti;
- Chiedere il permesso prima di scaricare dal web materiale di vario tipo.

GESTIONE ACCESSI (PASSWORD, BACKUP ECC.)

Accesso docenti

Ai docenti è consentito accedere ad Internet da propri dispositivi utilizzando la rete Wi-Fi dell'Istituto previa autorizzazione scritta del Dirigente.

La connessione Wi-Fi ad Internet dalla scuola è regolata da un meccanismo di autenticazione-autorizzazione:

- ✓ La persona fisica viene identificata e associata al MAC Andress del dispositivo con cui intende accedere ad Internet.
- ✓ L'accesso può avvenire unicamente da tale dispositivo.
- ✓ Il proprietario del dispositivo è l'unico responsabile di tutte le operazioni svolte con esso.
- ✓ In caso di furto o smarrimento del dispositivo identificato si deve immediatamente informare il personale tecnico incaricato che ne revocherà l'accesso alla rete.
- ✓ Il docente verificherà lo spegnimento della postazione al termine della sua ora di lezione.

Accesso studenti

Il Regolamento di Istituto vieta l'uso del cellulare.

In particolare, agli studenti **non** è consentito accedere ad Internet da propri dispositivi utilizzando la rete Wi-Fi dell'Istituto.

E-mail

Solo i docenti possono utilizzare i servizi mail accedendo alla rete della scuola a fini esclusivamente didattici.

Prima di aprire una mail è necessario pensare …

- ✓ **Spam**: email, messaggi istantanei e altre comunicazioni online indesiderate.
- ✓ **Phishing**: frode online per sottrarre con l'inganno numeri di carte di credito, password, informazioni su account personali.
- ✓ **Truffe**: email spedite da criminali che tentano di rubare denaro.

SITO WEB DELLA SCUOLA

Il Dirigente Scolastico e il personale incaricato di gestire le pagine del sito della Scuola hanno la responsabilità di garantire che il contenuto pubblicato sia accurato e appropriato.

La scuola offre all'interno del proprio sito una serie di servizi alle famiglie e ai fruitori esterni: i docenti che desiderano pubblicare attività didattiche dovranno chiedere l'autorizzazione al Dirigente.

SOCIAL NETWORK

Per la Legge l'utilizzo dei Social Network con la pubblicazione di nomi e giudizi sulle persone o sulle istituzioni e la diffusione di foto/filmati senza il consenso e, comunque, all'insaputa delle persone coinvolte può determinare ricadute di carattere anche penale, come ad esempio la diffamazione
Si invitano pertanto tutti gli studenti a non prelevare o diffondere immagini, video o registrazioni – anche solo audio – non autorizzate, ed eliminare da internet eventuali riferimenti offensivi o comunque illeciti (ed inopportuni) nei confronti dell'Istituto e dei suoi docenti e studenti.
Allo stesso tempo, si invitano gli allievi e i genitori a fare un uso prudente dei Social Network, in particolare Facebook e Whatsapp, limitandone l'uso alle sole comunicazioni funzionali, evitando ad ogni modo di esprimere giudizi sull'operato degli altri studenti o del personale della scuola, giudizi che una volta pubblicati comportano sempre una assunzione di responsabilità da parte di chi li ha scritti o anche semplicemente diffusi.
Si richiama l'attenzione sulla normativa e sulla regolamentazione dei social network che richiedono un età minima per la sottoscrizione (che al momento in cui si scrive è di 13 anni per Facebook e 16 anni per Whatsapp), pertanto la responsabilità ricade sui genitori dei minori che fruiscono di questi sevizi.

PROTEZIONE DEI DATI PERSONALI

Tutti i servizi offerti tramite il sito web della scuola, nel rispetto delle norme vigenti, non potranno ricondursi ad esempio, anche indirettamente, al trattamento dei dati personali sensibili o a dati giudiziari.

4.SRUMENTAZIONE PERSONALE

Per gli studenti: gestione degli strumenti personali-cellulari, tablet,ecc...
Come da regolamento d'istituto agli studenti è vietato l'utilizzo del cellulare o dello smartphone con funzione di telefono o per comunicazioni via messaggistica/social network all'interno della scuola. Per quanto concerne l'utilizzo dei tablet, questi possono essere utilizzati solo alla presenza del docente e per ragioni prettamente scolastiche.

Per i docenti e il personale della scuola: gestione degli strumenti personali-cellulari, tablet ecc...
I docenti e il personale della scuola possono usare cellulari e tablet a scopo personale non durante l'attività didattica o lavorativa e nei luoghi in cui non arrechino disturbo alla comunità scolastica.
Si richiama l'attenzione sulle conversazioni con le famiglie, che dovranno avvenire in un luogo riservato e protetto.

5.PREVENZIONE, RILEVAZIONE E GESTIONE DEICASI

La scuola è una comunità di dialogo, di ricerca, di esperienza sociale, informata ai valori democratici e volta alla crescita della persona in tutte le sue dimensioni. In essa ognuno, con pari dignità e nella diversità dei ruoli, opera per garantire la formazione alla cittadinanza, la realizzazione del diritto allo studio, lo sviluppo delle potenzialità di ciascuno e il recupero delle situazioni di svantaggio, in armonia con i principi sanciti dalla Costituzione e dalla Convenzione internazionale sui diritti dell'infanzia fatta a New York il 20 novembre 1989 e con i principi generali dell'ordinamento italiano DPR 24 giugno 1998, n.249.

PREVENZIONE

La Scuola ha scelto una politica interna che sia pro-attiva, tesa cioè a creare un ambiente di apprendimento sereno e sicuro in cui sia chiaro sin dal primo giorno di scuola che (cyber)bullismo, prepotenza, aggressione e violenza non sono permessi; in cui ci sia l'apertura necessaria all'incoraggiamento a parlare di sé e dei propri problemi, che stimoli alla partecipazione diffusa di tutta la comunità scolastica nelle azioni finalizzate al contrasto del cyberbullismo, che insegni ad interagire in maniera responsabile.

Contrastare il bullismo implica la creazione di una comunità solidale, in cui ogni allievo accetta sia il diritto di vivere una scuola senza violenza, sia la responsabilità di difendere i compagni più vulnerabili. Il coinvolgimento dei coetanei è indispensabile per creare un clima di solidarietà, combattere l'omertà e l'indifferenza, incoraggiare le vittime a chiedere aiuto, sottrarre al bullo i potenziali proseliti.

Rischi

I rischi a cui sono esposti gli allievi sono numerosi, la tabella elaborata dalla professoressa Menesini dell'Università di Firenze li rappresenta in modo molto efficace suddividendoli e classificandoli in base al comportamento del ragazzo

	Contenuto Ragazzo destinatario di produzioni di massa	**Contatto** Ragazzo come partecipante (attività iniziate da adulti)	**Condotta** Ragazzo è attore (sia come vittima che come attore)
Aggressivo	**Violenza / contenuti cruenti**	**Molestie, stalking**	**cyberbullismo**
Sessuale	**Pornografia**	**Grooming, richieste sessuali**	**Molestare sessualmente Sexting**
Valori	**Razzismo/odio**	**Persuasione ideologica**	**Autolesionismo anoressia**
Commerciale	**Vendita e sfruttamento**	**Violazione della privacy/ abuso di dati personali**	**Scaricare Gioco d'azzardo**

sull'asse orizzontale e al tipo di rischio a cui è sottoposto sull'asse verticale.www.centrorisorseausili.it/Varie/2016_03_19%20CTS%20Empoli_Menesini.pdf

Gli allievi sono potenzialmente esposti a tutti i rischi descritti, la Scuola quindi deve prenderli in considerazione tutti e pianificare azioni di prevenzione del rischio, rilevazione e gestione dei casi.

Azioni

Premesso che non ci sono ricette sicure per eliminare il cyberbullismo, la Scuola ha scelto di impegnarsi su più fronti per essere zona libera da cyberbullismo, e nel corso dell'anno scolastico sono state realizzate le seguenti azioni:

1. peer education: il gruppo dei Peer-Z, quattordici alunni delle classi seconde e terze formati da educatori all'interno del progetto "Generazioni connesse", seguiti e sostenuti dal referente cyberbullismo d'istituto , ha effettuato nel corso dell'anno scolastico interventi in tutte le classi della sede "Boifava", interverrà l'anno prossimo in tutte le classi prime e, con il supporto del docente di riferimento, passerà il testimone ad un nuovo gruppo di peer educator.
2. elaborazione di attività a cura dei docenti da proporre nelle classi: il gruppo di docenti che ha aderito al progetto "Generazioni connesse" ha sviluppato alcune proposte disponibili nel sito del progetto.
3. ricerca di interventi promossi a titolo gratuito dal territorio:

a. progetto "Cuoriconnessi" della Polizia postale italiana per alcune classi terze e seconde della sede "Boifava";

b. interventi della polizia di Stato per le classi seconde della sede "Boifava";

c. interventi del dott. Picchio in qualità di Formatore cyberbullismo per le classi terze delle scuola media "Boifava";

d. Progetto "Attenti al gruppo" tenuto da Psicologi del Consultorio familiare "Beretta Molla di Milano per le classi Prime e Seconde;

1. Interventi da parte del Referente Cyberbullismo d'Istituto:

a. Formazione diretta con le classi Prime sulle conoscenze di base del fenomeno del Cyberbullismo

b. Applicazione della metodologia "Tripax" in alcune classi più a rischio.

c. Vari Progetti sportivi finalizzati in particolare all'inclusione scolastica e al miglioramento delle relazioni tra pari.

Nel corso del prossimo anno scolastico la Scuola intende:

1. proseguire l'attività di peer education come indicato sopra;
2. proporre a tutte le classi con il supporto dei docenti del gruppo di progetto "Generazioni connesse" le attività elaborate quest'anno.
3. riproporre attività gratuite con esperti esterni ricercati sul territorio
4. elaborare un proposta di approccio curricolare inserendo attività di sensibilizzazione nell'azione didattica da svolgere in classe a cura dei docenti utilizzando filmati (ad esempio Gaetano per le classi prime, Inside out per le classi seconde, La solitudine dei numeri prime per le classi terze), episodi di cronaca recenti o testi come stimolo per la discussione in classe, l'acquisizione di consapevolezza del problema, delle motivazioni sottostanti e delle conseguenze e la promozione di un sistema di regole e di una cultura anti prepotenze nella classe. (www.centrorisorseausili.it/Varie/2016_04_07%20CTS%20Empolese_Palladino.pdf)
5. analizzare la possibilità di attivare programmi di intervento EvidenceBased come "No Trap (Noncadiamointrappola!) – liberi dal bullismo"(www.notrap.it).
6. promuovere la diffusione della conoscenza delle Linee di orientamento per azioni di prevenzione e di contrasto al bullismo e al cyberbullismo del MIUR.
7. implementare la e-Safety Policy con il contributo di tutte le componenti (docenti, studenti,

famiglie, personale A.T.A.).

8. presentare la e- Safety Policy così redatta agli Organi Collegiali e quindi inserirla nel sistema di regolamenti della Scuola e renderla pubblica sul sito della Scuola.

RILEVAZIONE

Che cosa segnalare

Le tipologie di comportamenti online da segnalare sono:

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

Come accorgersi se un alunno/un'alunna è coinvolto/a in casi di cyberbullismo?

Accorgersi di episodi di cyberbullismo non è sempre facile perché le prevaricazioni avvengono in luoghi virtuali in cui gli adolescenti si ritrovano. Per cui 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 è opportuno tenere presenti alcuni indicatori che ci possono aiutare per verificare se nella classe sono presenti episodi di prevaricazione. Esempi di domande stimolo utili per arrivare all'identificazione del problema sono presenti nei materiali di supporto dell'area scuole del sito generazioni connesse (6.1.1agire).

Come segnalare: con quali strumenti e a chi

- La scuola ha previsto i seguenti strumenti per far uscire allo scoperto il problema:
- la"**bluebox**": quest'anno abbiamo sperimentato questa strategia per eventuali segnalazioni in collaborazione con la Polizia di Stato.
- il "**counselling**": il Referente Bullismo/Cyberbullismo che mette la propria competenza al servizio dei ragazzi, fornendo ascolto a tutte le richieste degli alunni.
- Il gruppo dei "**Peer-Z**": alunni appositamente formati, che potranno avere la funzione di supporto e di aiuto tra pari.
- la Metodologia "**Tripax"(** un efficace metodo europeo per prevenzione e contrasto di bullismo e cyberbullismo) che consente non solo di individuare eventuali Bulli/Cyberbulli e Vittime ma soprattutto di educare i ragazzi all'empatia sin dalla Scuola Primaria

Una volta rilevato il fatto, cosa deve fare la Scuola?

Per questo la nostra Scuola opererà una politica di intervento sia **reattiva** che **pro-attiva.** Quella **reattiva** dovrà prevedere azioni di supporto al cyberbullo perché compia un processo di maturazione che lo porti a comprendere che qualsiasi forma di sopraffazione non è accettabile. Quella **proattiva**, richiede la partecipazione di tutte le componenti della comunità scolastica e dovrà essere rivolta a insegnare a tutti, potenziali bulli e vittime, sia come essere assertivi, sia come saper gestire la propria aggressività e istinto di sopraffazione, promuovendo un'interazione tra pari più responsabile.

Come gestire le segnalazioni

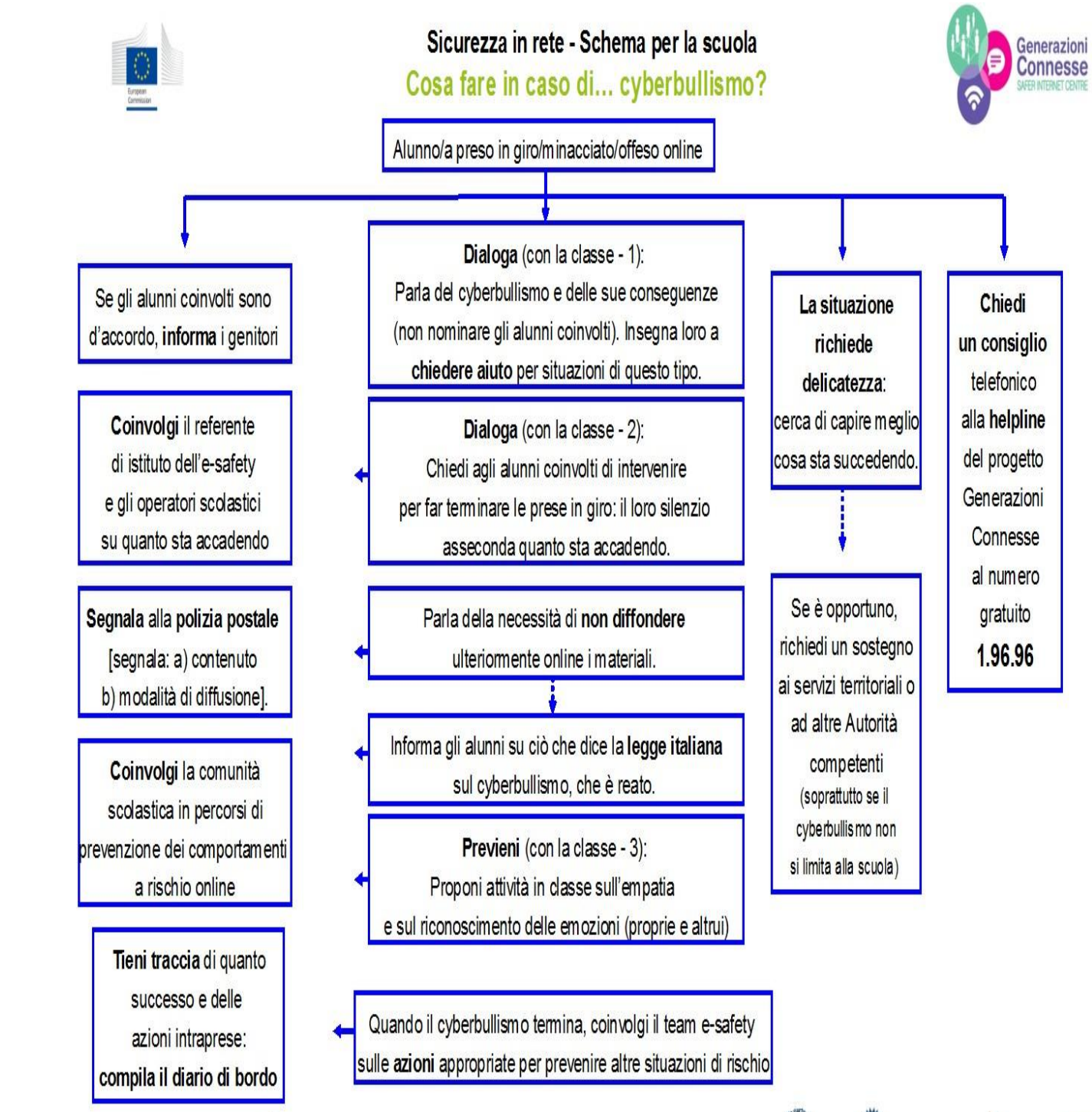
Le tappe da seguire quando si presenta un caso di cyberbullismo sono:

- 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.

Come già detto per la prevenzione, 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.

  La Scuola in quanto comunità scolastica solidale si dichiara contraria ad ogni forma di cyberbullismo. Perciò verrà proposta e condivisa la procedura descritta nel seguente schema:


Sicurezza in rete - Schema per la scuola
Cosa fare in caso di... cyberbullismo?
Generazioni Connesse
SAFER INTERNET CENTRE
Alunno/a preso in giro/minacciato/offeso online
Se gli alunni coinvolti sono d'accordo, informa i genitori
Coinvolgi il referente di istituto dell'e-safety e gli operatori scolastici su quanto sta accadendo
Segnala alla polizia postale [segnala: a) contenuto b) modalità di diffusione].
Coinvolgi la comunità scolastica in percorsi di prevenzione dei comportamenti a rischio online
Tieni traccia di quanto successo e delle azioni intraprese: compila il diario di bordo
Dialoga (con la classe - 1): Parla del cyberbullismo e delle sue conseguenze (non nominare gli alunni coinvolti). Insegna loro a chiedere aiuto per situazioni di questo tipo.
Dialoga (con la classe - 2): Chiedi agli alunni coinvolti di intervenire per far terminare le prese in giro: il loro silenzio asseconda quanto sta accadendo.
Parla della necessità di non diffondere ulteriormente online i materiali.
Informa gli alunni su ciò che dice la legge italiana sul cyberbullismo, che è reato.
Previeni (con la classe - 3): Proponi attività in classe sull'empatia e sul riconoscimento delle emozioni (proprie e altrui)
Quando il cyberbullismo termina, coinvolgi il team e-safety sulle azioni appropriate per prevenire altre situazioni di rischio
La situazione richiede delicatezza: cerca di capire meglio cosa sta succedendo.
Se è opportuno, richiedi un sostegno ai servizi territoriali o ad altre Autorità competenti (soprattutto se il cyberbullismo non si limita alla scuola)
Chiedi un consiglio telefonico alla helpline del progetto Generazioni Connesse al numero gratuito 1.96.96
© All rights reserved Generazioni connesse 2015

E’ previsto anche un monitoraggio costante dei casi segnalati, da realizzare attraverso un diario di bordo da compilare con regolarità.

Schema riepilogativo delle situazioni gestite legate a rischi online

Riepilogo casi

Scuola_____ Anno Scolastico_____

N°	Data	ora	Episodio (riassunto)	Azioni intraprese		Insegnante con cui l'alunno/a si è confidato	Firma
				Cosa?	Da chi?		

© All rights reserved Generazioni Connesse 2015

LINEE GUIDA PER UNA SCUOLA LIBERA DACYBERBULLISMO

LINEE GUIDA PER I RAGAZZI

Consigli per difendersi dai rischi legati all'uso delle nuove tecnologie

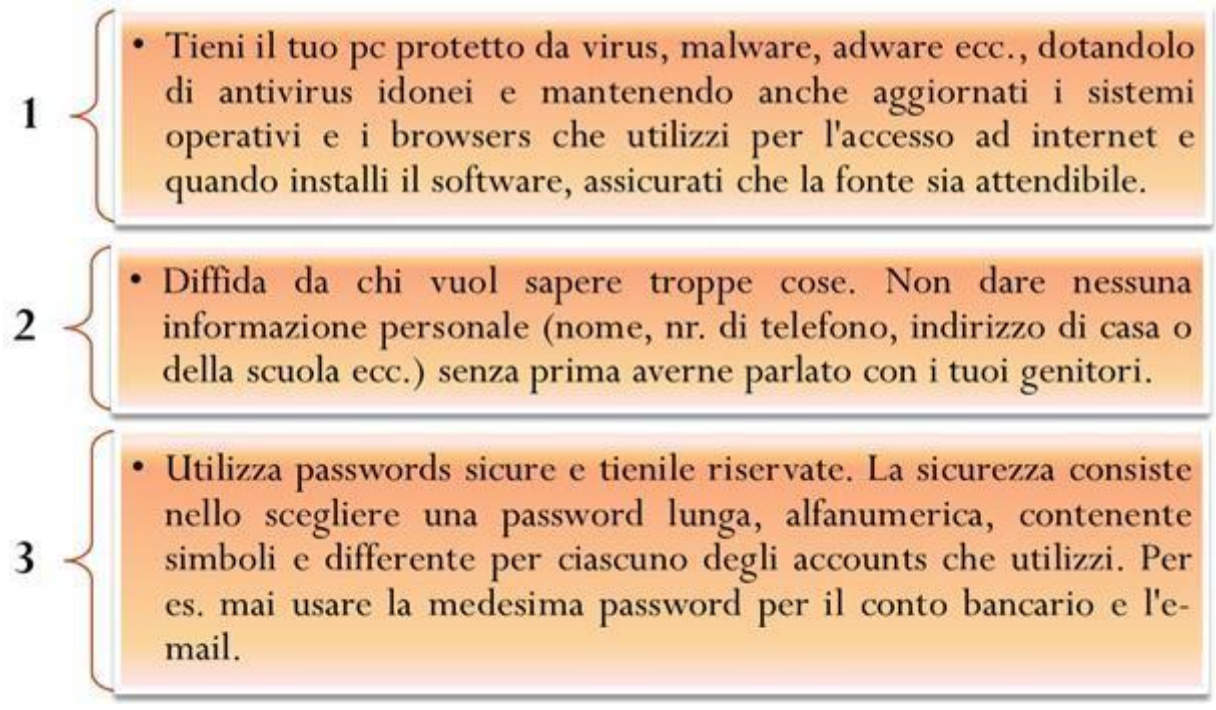
Il cyber bullismo (ossia "bullismo" online) è il termine che indica atti di bullismo e di molestia effettuati tramite e-mail, sms, blog, social network e internet.

La forma online del bullismo ha alcune caratteristiche che la rendono particolarmente pericolosa perché:

1. il cyberbullismo è pervasivo: il cyberbullo può raggiungere la vittima in qualsiasi luogo e in qualsiasi momento;
2. è un fenomeno persistente: il materiale diffamatorio può rimanere disponibile per molto tempo;
3. spettatori e cyberbulli sono potenzialmente infiniti;
4. i protagonisti sono diversi: il cyberbullo può essere anche una persona estranea, può agire singolarmente o in gruppo e può, se vuole, rimanere anonimo o protetto da un avatar o da un nickname.

Tutti quelli che osservano senza far nulla diventano corresponsabili delle azioni del cyberbullo; mettere un "like" su un social o condividere o commentare foto o video sottopone chi lo fa a una responsabilità maggiore.

La Rete può essere un posto fantastico ma dipende anche da te...



4

- Ricordati sempre che è facile mentire quando si è online: alcune persone possono fingersi quello che non sono realmente. Non è una buona idea incontrare qualcuno che si è conosciuto solo tramite la Rete, anche se questa persona ti ha inviato una sua foto o si è presentata attraverso una webcam. Ogni immagine sul web può essere falsa. Informa sempre i genitori prima di avventurarti in incontri con persone conosciute via Internet.

5

- Attenzione ai falsi ed evita le truffe. Non rispondere a messaggi istantanei o e-mails che ti chiedono dati personali, passwords o numero di carta di credito, cestinale subito senza aprire gli eventuali allegati che potrebbero essere dannosi o contenere materiale non idoneo a bambini e adolescenti. Evita di entrare in siti "a pagamento".

6

- Se si ricevono messaggi o si incontrano contenuti che mettono a disagio, non cercare di saperne di più da solo, segnalalo ai genitori, agli insegnanti o ad un adulto di cui ti fidi.

7

- Su social networks, chatrooms, forum, blog con allegria e prudenza. Se qualcuno crea disturbi, mette a disagio, suggerisce argomenti di discussione che imbarazzano o spaventano, è bene bloccarlo immediatamente interrompendo ogni contatto. Non continuare la conversazione se non ti senti a tuo agio.

8

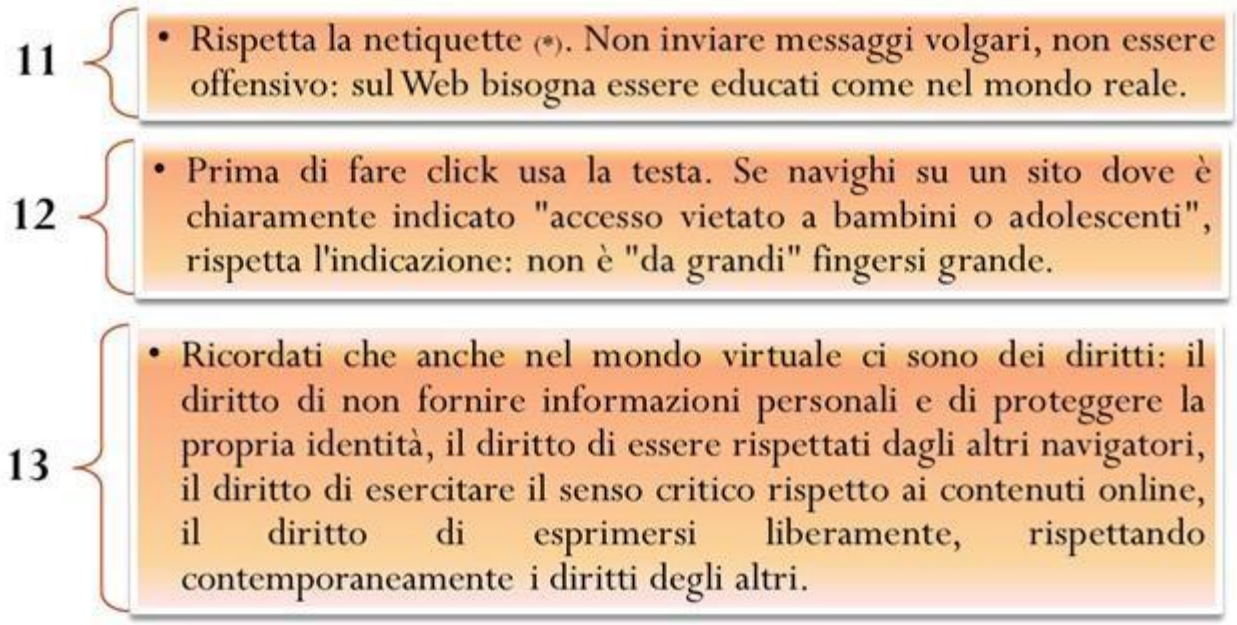
- Pensa a ciò che pubblichi su Internet. Sii consapevole della tua reputazione digitale evitando la pubblicazione di contenuti imbarazzanti, dannosi o inappropriati e non utilizzare la webcam vestito in modo succinto e/o assumendo un comportamento inopportuno, potresti essere manipolato o minacciato.

9

- Presta particolare attenzione alle registrazioni online, verifica che l'indirizzo web inizi con https://. La s indica che la connessione al sito è crittografata e quindi più sicura.

10

- Blocca sempre lo schermo quando non utilizzi il pc, il tablet o il telefono o, per maggior sicurezza, imposta il blocco automatico dopo un tot. di tempo che risultano inutilizzati.



LINEE GUIDA PER I GENITORI

Consigli per difendere i propri figli dai pericoli legati all'uso delle nuove tecnologie

Molti bambini utilizzano internet già durante i primi anni della scuola primaria (6-7 anni). È importante sottolineare che è fondamentale l'accompagnamento all'utilizzo di internet da parte di un adulto (genitore, insegnante, educatore) in relazione all'età del bambino.

I bambini al di sotto dei 10 anni, in genere, non avendo ancora sviluppato le capacità di pensiero critico necessarie, non sono in grado di esplorare il web da soli.

Con la preadolescenza e l'adolescenza si intensifica l'uso di Internet: i giovani scaricano musica, utilizzano motori di ricerca per trovare informazioni, visitano siti, inviano e ricevono sms, la posta elettronica e i giochi online. La supervisione degli adulti è quindi fondamentale anche in questa fase, poiché una maggior conoscenza e consapevolezza legate alla crescita non mettono comunque al riparo dai rischi della Rete.

Ricordatevi che…

Per vostro figlio la protezione non è data solo da "FILTRI" da applicare al computer: è fondamentale, invece, il dialogo costante e continuo, la vicinanza e la partecipazione alle problematiche dei vostri ragazzi.

1. • Imparate a navigare in internet per capire che non è possibile adottare mezzi di difesa e di controllo se non possedete una minima cultura informatica.

2. • Chiedete ai vostri figli di essere informati rispetto alle loro attività online: che cosa fanno in Rete e con chi stanno comunicando.

3. • Stabilite i tempi di utilizzo del computer e del collegamento in Rete a seconda dell'età di vostro figlio. Si può considerare eccessivo un utilizzo che sottrae tempo alle altre attività importanti per la crescita (studio, amici, sport, socializzazione nel mondo reale).

4. • Condividete le raccomandazioni per un uso sicuro di Internet con i vostri figli. È utile scrivere insieme a loro una "carta delle regole di comportamento" e magari appenderla di fianco al computer.

5. • Mettete il computer in una stanza di accesso comune, non nella camera dei ragazzi o in un ambiente isolato. Internet va considerato come uno strumento utile per tutta la famiglia.

6. • Se non potete seguire direttamente la navigazione dei vostri figli, potete utilizzare dei software di protezione per monitorare l'uso di internet e dei software "filtro" per veicolare la navigazione solo verso siti consentiti. Controllate periodicamente il contenuto dell'hard disk e verificate la cronologia dei siti web visitati dai vostri ragazzi.

7. • Spiegate ai vostri figli che le persone che incontrano in Rete non sempre sono quello che dicono di essere.

8. • Parlate apertamente con i vostri figli dei rischi che possono presentarsi durante la navigazione. I ragazzi devono essere consci dei pericoli ai quali vanno incontro e sapere che possono confidarsi con i genitori in caso di brutti incontri virtuali.

9 • Insegnate ai vostri figli a bloccare chi li infastidisce in Rete.

10 • Spiegate ai vostri figli che non bisogna mai fornire online dati personali a sconosciuti (nome, età, indirizzo, nr. telefono, e-mail, messanger id, foto proprie e/o di familiari e amici) e non bisogna inviare a nessuno informazioni bancarie e/o compilare moduli online dove vengano richieste.

11 • Se i ragazzi ricevono sulla propria casella di posta elettronica spam, posta pubblicitaria e messaggi da mittenti sconosciuti, occorre dire loro di eliminarli senza aprirne gli allegati: potrebbero infatti contenere virus, malware ecc. in grado di danneggiare il computer o materiale non adatto ai minorenni.

12 • Dimostrate ai vostri figli la disponibilità ad ascoltarli, anche per fornire loro l'opportunità di riferire se qualcuno o qualcosa li ha turbati o li ha fatti sentire a disagio durante la navigazione.

13 • Insegnate ai vostri ragazzi che comportamenti illeciti nel mondo reale (per es. insultare una persona, sottrarre credenziali ad un amico, accedere illecitamente ad un sito o ad un servizio ecc.), sono illegali anche in Rete.

14 • Considerate che spesso, navigando, ci si allontana molto dal punto da cui si è partiti per effettuare una ricerca: questo aumenta il rischio di accedere anche involontariamente a materiali non idonei a bambini e adolescenti; è perciò necessaria una vostra continua attenzione.

LINEE GUIDA PER LA SCUOLA

Suggerimenti per prevenire il cyberbullismo e promuovere un uso critico della rete tra gli studenti

È proprio nel mondo della scuola che il bullismo, il più delle volte, si genera e si manifesta: il bullo attua le sue prepotenze e la vittima vive il suo dramma, facendo sì che l'esperienza scolastica acquisisca una connotazione negativa che va ad influire sul normale sviluppo dei soggetti coinvolti. I giovani, siano essi bulli o vittime, difficilmente parlano o si sfogano con gli adulti di quello che succede loro, gli uni per non essere scoperti e gli altri per paura di peggiorare la loro situazione.

Ecco perché la scuola rappresenta il luogo migliore in cui poter iniziare a fare prevenzione e in cui promuovere sia una cultura pro-sociale che veda, nell'altro diverso da sé, solo un altro modo di essere, né migliore, né peggiore, sia una cultura del confronto e del dialogo aperto, dove apprendere che il bullismo è un comportamento sbagliato e che solo parlandone lo si può riconoscere e sconfiggere.
La scuola, così come i genitori, ha il compito di guidare il ragazzo ad acquisire competenza e quindi anche una buona sicurezza, valorizzandolo ed apprezzando le sue qualità personali positive.

1. Conoscere Internet significa anche dimostrare ai ragazzi di essere vicini al loro mondo. È necessario quindi che teniate sempre aggiornate le vostre competenze tecnologiche.
2. Cercate di capire il livello delle conoscenze informatiche degli studenti ed organizzate eventualmente qualche ora di formazione.
3. Informate gli alunni sui rischi presenti in Rete, senza demonizzarla, ma sollecitandone un utilizzo consapevole, in modo che Internet possa rimanere per i ragazzi una fonte di divertimento e apprendimento.
4. Educate bambini e adolescenti alla prudenza, a non fornire dati ed informazioni personali, ad abbandonare un sito dai contenuti che possono turbare o spaventare e a non incontrare persone conosciute in Rete senza averne prima parlato con i genitori.
5. Mostrate agli studenti come usare e valutare criticamente ciò che incontrano durante la navigazione: non tutte le informazioni online sono affidabili.
6. Spiegate agli alunni che comportamenti illeciti nel mondo reale (per es. insultare una persona, sottrarre credenziali ad un amico, accedere illecitamente ad un sito o a un servizio ecc.), lo sono anche in Rete. .

Milano, 17 maggio 2018

Il Dirigente Scolastico
(prof.ssa Maria Paola Tirone)

Il Referente per il bullismo e cyberbullismo
(prof. Francesco Rosa)

Milano, 13 giugno 2018

Il Presidente del Consiglio d'Istituto
(sig.ra Cristina Pinnavaia)