Ministero dell'Istruzione, dell'Università e della Ricerca

**I.C. GARIBALDI**

Via Marconi 46 20092 Cinisello Balsamo (MI)
Tel. 02 61294190 Fax 02 6184181
Cod. Fisc. 94581370155 Cod. Min. MIIC8AR001
e-mail miic8ar001@istruzione.it miic8ar001@pec.istruzione.it
Codice Univoco UFRWPT


# E-Safety Policy

***Anno scolastico 2022/23***

INDICE DEI CONTENUTI

## 1. Introduzione

### *1.1 Scopo della Policy*

La presente Policy costituisce un documento regolativo per tutti i membri della comunità scolastica che hanno accesso ai sistemi informatici della scuola, con lo scopo di dare indicazioni per l'uso corretto e responsabile delle apparecchiature di cui essa dispone.

In particolare viene redatta sia per regolare il comportamento degli studenti dentro le aule e nell'aula informatica sia per educarli ad adottare buone pratiche comportamentali nell'uso della rete, onde evitare che fenomeni di cyberbullismo si possano verificarsi dentro e/o fuori l'ambiente scolastico. A tal fine la scuola promuove azioni che limitino l'accesso a siti e ad applicazioni illeciti e conferisce ai docenti la responsabilità di guidare gli studenti nelle attività online, indicando loro regole di condotta chiare per un uso critico e consapevole di Internet anche a casa.

Ciò premesso essa autorizza il personale docente a erogare sanzioni disciplinari per comportamenti inappropriati avvenuti all'interno dell'istituzione scolastica ed estende tale controllo anche a quelli che possono avvenire al di fuori ma sono legati alla frequenza della stessa. Attraverso la prevenzione, il controllo e la formazione si intende così ridurre al minimo, se non scongiurare, l'insorgere di atti che possano creare disagio nelle relazioni tra alunni o che addirittura potrebbero configurarsi come reato.

### *1.2 Ruoli e responsabilità (che cosa ci si aspetta da tutti gli attori della comunità scolastica)*

Fermo restando quanto stabilito e riportato nel Regolamento d'Istituto, la presente e-Policy intende sottolineare quanto segue con lo scopo di indicare, per ogni componente scolastica, linee guida chiare e finalizzate ad un uso critico, sicuro e consapevole di Internet.

**Il dirigente scolastico:**

- coinvolge, nella prevenzione e contrasto al fenomeno del cyberbullismo, tutte le componenti della comunità scolastica, particolarmente quelle che operano nell'area dell'informatica, partendo dall'utilizzo sicuro di Internet a scuola;
- individua attraverso il Collegio dei Docenti un referente del bullismo e cyberbullismo;
- prevede all'interno del PTOF corsi di aggiornamenti e formazione in materia di prevenzione del cyberbullismo, rivolti al personale docente ed Ata;
- promuove sistematicamente azioni di sensibilizzazione sul fenomeni del cyberbullismo in rete con enti, associazioni, istituzioni locali ed altre scuole, coinvolgendo alunni, docenti, genitori ed esperti;
- favorisce la discussione all'interno della scuola, attraverso i vari organi collegiali, creando i presupposti di regole condivise di comportamento per il contrasto e prevenzione del fenomeno del cyberbullismo;
- prevede azioni culturali ed educative rivolte agli studenti, per acquisire le competenze necessarie all'esercizio di una cittadinanza digitale consapevole;
- garantisce una formazione adeguata del personale docente relativo all'uso delle TIC nella didattica;
- garantisce 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;
- garantisce l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line;
- segue 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.

**L'animatore digitale:**

- favorisce la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornisce consulenza e informazioni al personale in relazione ai rischi on line e alle misure di prevenzione e gestione degli stessi;
- rileva le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola;
- assicurare che gli utenti possano accedere alla rete della scuola solo tramite password;
- cura la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti (istruzione e formazione);
- coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti alla "scuola digitale";
- assicura la massima diffusione della e-policy dentro la comunità scolastica e in tutte le sue componenti (docenti/ata, genitori e studenti), mediante pubblicazione sul sito della scuola

**Il referente del "bullismo e cyberbullismo":**

- promuove la conoscenza e la consapevolezza dei rischi connessi al bullismo e al cyberbullismo attraverso progetti d'istituto che coinvolgano genitori, studenti e tutto il personale;
- coordina le attività di prevenzione ed informazione sulle sanzioni previste e sulle responsabilità di natura civile e penale, anche con eventuale affiancamento di genitori e studenti;
- si rivolge a partner esterni alla scuola, quali servizi sociali e sanitari, aziende del privato sociale, forze di polizia, per realizzare un progetto di prevenzione;
- cura rapporti di rete fra scuole per eventuali convegni/seminari/ corsi e l'organizzazione della giornata mondiale sulla Sicurezza in Internet, la "Safer Internet Day".
- collabora in team con altre figure scolastiche (Animatore Digitale e Team per l'Innovazione; Referente BES/Inclusione; Referente per la Dispersione);
- Segnala tempestivamente situazioni di rischio online o casi di bullismo o cyberbullismo; supporta i Consigli di Classe ed i Coordinatori;
- Facilita la formazione e la consulenza di tutto il personale; raccoglie e diffonde buone pratiche educative, organizzative e azioni di monitoraggio.

**Commissione bullismo e cyberbullismo:**

- cura la redazione e la revisione annuale della policy sulla base delle osservazioni ricevute da tutti i soggetti interessati;
- all'interno della scuola e in riferimento ai diversi ordini scolastici e alle diverse collocazioni territoriali dei plessi, garantire la comunicazione (sportello, circolari, sito web, ecc.) e il funzionamento di ogni mezzo e attività connessa all'uso corretto della TIC;
- coordina, nei diversi plessi, le attività relative alla prevenzione del fenomeno del bullismo e del cyberbullismo;
- riferisce al Dirigente Scolastico situazioni o problemi di particolare rilevanza su cui intervenire;
- concorda modalità e tempi per favorire un equo sviluppo delle risorse digitali in tutti i plessi e in tutti gli ordini scolastici dell'istituto;
- si adopera per allargare quanto più possibile una "rete" che coinvolga al suo interno le diverse componenti scolastiche.

**Il direttore dei servizi generali e amministrativi:**

- assicura, 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;

**Personale ATA:**

- segnala qualsiasi abuso, anche sospetto, al Dirigente Scolastico o all'animatore digitale per le opportune indagini / azioni / sanzioni;
- mantiene tutte le comunicazioni digitali con alunne/alunni e genitori/tutori a livello professionale e le realizza esclusivamente con sistemi ufficiali scolastici;

**Il collegio docenti:**

- promuove scelte didattiche ed educative, anche in collaborazione con altre scuole in rete, per la prevenzione del fenomeno del cyberbullismo e per la diffusione di pratiche corrette nell' uso di internet.

**Il consiglio di classe:**

- pianifica attività didattiche e/o integrative finalizzate al coinvolgimento attivo e collaborativo degli studenti e all'approfondimento di tematiche che favoriscano la riflessione e la presa di coscienza del necessario rispetto dei valori di convivenza civile, anche nell'uso dei social network.

**Il docente:**

- intraprende azioni congruenti con l'utenza del proprio ordine di scuola, tenuto conto che l'istruzione ha un ruolo fondamentale sia nell'acquisizione e rispetto delle norme relative alla convivenza civile, sia nella trasmissione dei valori legati ad un uso responsabile di internet;
- valorizza nell'attività didattica modalità di lavoro di tipo cooperativo e spazi di riflessioni adeguati al livello di età degli alunni, all'interno dei quali:
- illustra ai propri alunni le regole di utilizzo contenute nel presente documento;
- dà chiare indicazioni sul corretto utilizzo della rete (Internet, piattaforma studenti ecc);
- si assume la responsabilità di segnalare prontamente eventuali malfunzionamenti o danneggiamenti al tecnico informatico;

**Inoltre**

non si allontana dalla postazione, lasciandola incustodita, se non prima di aver effettuato la disconnessione;

non salva sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili.

**Gli alunni:**

- sono coinvolti nella progettazione e nella realizzazione delle iniziative scolastiche, al fine di favorire un miglioramento del clima relazionale;
- imparano le regole basilari per rispettare gli altri quando sono connessi alla rete, facendo attenzione alle comunicazioni (email, sms, mms) che inviano;
- durante le attività didattiche o comunque all'interno della scuola, possono acquisire, mediante telefoni cellulari o altri dispositivi elettronici, immagini, filmati o registrazioni vocali, solo per finalità didattiche, previo consenso del docente. La divulgazione del materiale acquisito all'interno dell'istituto è utilizzabile solo per fini esclusivamente personali di studio o documentazione e comunque nel rispetto del diritto alla riservatezza di tutti;
- durante le lezioni o le attività didattiche in genere non possono usare cellulari, giochi elettronici e riproduttori di musica, se non per finalità didattiche, previo consenso del docente;
- in caso di riscontro di malfunzionamenti della strumentazione e/o di contatto accidentale con informazioni, immagini e/o applicazioni inappropriate lo comunicano immediatamente all'insegnante;
- non possono eseguire tentativi di modifica della configurazione di sistema delle macchine.

**I genitori**:

- partecipano alle azioni di formazione/informazione istituite dalle scuole, relativamente ai comportamenti sintomatici del bullismo e del cyberbullismo;
- sono attenti ai comportamenti dei propri figli;
- vigilano sull'uso delle tecnologie da parte dei ragazzi, con particolare attenzione ai tempi, alle modalità, agli atteggiamenti conseguenti;
- conoscono le azioni messe in campo dalla scuola e collaborano secondo le modalità previste dal Patto di corresponsabilità;
- conoscono il codice di comportamento dello studente;
- conoscono le sanzioni previste dal regolamento d'istituto nei casi di bullismo, cyberbullismo e navigazione online a rischio.

*1.3 . Condivisione e comunicazione della Policy all'intera comunità scolastica*

La E- Policy sarà pubblicata nel sito della scuola.

All'inizio di ogni anno scolastico, insieme al Patto di Corresponsabilità Educativa, la E-Policy verrà illustrata ai genitori e agli alunni dell'istituto comprensivo.

*1.4. Gestione delle infrazioni alla Policy*

La gestione dei casi rilevati va differenziata a seconda della loro gravità; fermo restando che è opportuna la condivisione a livello di Consiglio di Classe di ogni episodio rilevato, anche minimo, alcuni avvenimenti possono essere affrontati e risolti con la discussione collettiva in classe. Altri casi ancora possono essere affrontati convocando genitori e alunno/a per riflettere insieme su quanto accaduto e su come rimediare. Nei casi più gravi e in ogni ipotesi di reato occorre valutare tempestivamente con il Dirigente Scolastico come intervenire.

Le infrazioni alla Policy possono essere rilevate da docenti/ATA nell'esercizio delle proprie funzioni oppure possono essere segnalate da alunni e genitori a docenti/ATA. Qualora esse si configurino come vero e proprio reato ( nella specie di minaccia, induzione alla prostituzione minorile, pedopornografia, corruzione di minorenne), occorre darne tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso. Se le infrazioni della Policy violano norme previste dal Regolamento d' Istituto si procede secondo quanto previsto dal Regolamento stesso .

1. Segnalazione > genitori, insegnanti, alunni
2. Equipe anti-bullismo →Dirigente → consiglio d'Istituto
3. Raccogliere informazioni / verificare/ valutare →prof. principale
4. Interventi con Soggetti coinvolti: Equipe anti-bullismo, Alunni, Genitori, Professori, Psicologa, Sportello d'ascolto.
5. Interventi: Incontri con gli alunni coinvolti, discussione in classe - Informare e coinvolgere genitori - Responsabilizzare gli alunni –(ri)stabilire regole di comportamento /di classe - Counselling (sportello) - (adattamento delle) misure -Trasferimento a un'altra classe
6. Sanzioni/ misure :
   I provvedimenti disciplinari devono prevedere anche comportamenti attivi di natura " riparatoria-risarcitoria". La sanzione deve orientarsi verso una responsabilizzazione del discente all'interno della comunità di cui è parte. Comportamenti volti a "riparare" il danno arrecato.
   - Lettera di scuse da parte del bullo
   - Scuse in un incontro con la vittima
   - Compito sul bullismo.
   - Intervento CdC per eventuale allontanamento dalla scuola.
7. Valutazione

Se il problema è risolto: rimanere attenti

Se la situazione continua: proseguire con gli interventi.

*1.5. Monitoraggio dell'implementazione della Policy e suo aggiornamento*

La presente Policy sarà riesaminata annualmente o quando si verificano cambiamenti significativi per quanto riguarda le tecnologie in uso nella scuola o le scelte operative e normative per la repressione del fenomeno del bullismo e cyberbullismo.

Tutti i cambiamenti saranno discussi e condivisi dalla comunità scolastica

*1.6. Integrazione della Policy con Regolamenti esistenti*

La presente Policy sarà allegata in appendice al Regolamento d'Istituto .

1.7 Linee guida per la Didattica digitale integrata

Le linee guida sono state anche inviate alle scuole per la loro applicazione.

La DDI (**Didattica Digitale Integrata**) è una modalità organizzativa che alterna momenti in presenza e momenti online. Il Ministero dell'Istruzione ha pubblicato sul proprio sito le Linee Guida per la Didattica Digitale Integrata (DDI), previste dal Piano per la ripresa di settembre presentato lo scorso 26 giugno e passate al vaglio del Consiglio Superiore della Pubblica Istruzione. Il documento contiene indicazioni operative affinché ciascun Istituto scolastico possa dotarsi, capitalizzando l'esperienza maturata durante i mesi di chiusura, di un Piano scolastico per la didattica digitale integrata. In particolare, il Piano per la DDI dovrà essere adottato nelle secondarie di secondo grado anche in previsione della possibile adozione, a settembre, della didattica digitale in modalità integrata con quella in presenza. Mentre dall'infanzia alla secondaria di primo grado, il Piano viene adottato affinché gli istituti siano pronti "qualora si rendesse necessario sospendere nuovamente le attività didattiche in presenza a causa delle condizioni epidemiologiche contingenti".

Per questi gradi di scuola non è infatti prevista didattica integrata alla ripresa di settembre, ma solo didattica in presenza.

## 2. Formazione e Curricolo

*2.1. Curricolo sulle competenze digitali per gli studenti*

Lo sviluppo delle competenze digitali e in generale della consapevolezza digitale è fondamentale all'interno dell'odierna struttura socio-economica.

La scuola ha il dovere di: sviluppare competenze digitali e rendere fruibili le apparecchiature informatiche come parte integrante dell' esperienza di apprendimento.

L'uso delle TIC va inserito pertanto nel curricolo sia a livello disciplinare sia a livello interdisciplinare.

In particolare il curricolo dovrà essere strutturato al fine di prevedere:

- insegnare ciò che è accettabile nell'utilizzo di Internet e ciò che è vietato, fornendo strumenti per l'utilizzo efficace di Internet e la conoscenza delle conseguenze delle violazioni;
- mostrare come produrre, pubblicare e presentare contenuti digitali in modo appropriato, sia in ambienti privati sia in ambienti condivisi;
- insegnare la valutazione dei contenuti Internet;
- impiegare materiali prelevati da Internet a scopi didattici conformemente al diritto d'autore;
- rendere alunne e alunni criticamente consapevoli dei materiali che si leggono sul web allo scopo di vagliare le informazioni prima di accettarne la fondatezza, la coerenza, le origini;
- mostrare la segnalazione di contenuti Internet sgradevoli o illegali.

Inserita nelle otto Competenze chiave di cittadinanza attiva indicate dal Consiglio di Lisbona nel marzo 2000, la Competenza digitale viene così definita all'interno della Raccomandazione del Parlamento europeo e del Consiglio del 18 dicembre 2006, relativa a competenze chiave per l'apprendimento permanente (2006/962/CE):

La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione per il lavoro, il tempo libero e la comunicazione. Essa è supportata da abilità di base nelle TIC: l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite internet.

La Competenza digitale è trasversale alle discipline previste dalle Indicazioni Nazionali 2012;
in tutte le discipline si ritrovano abilità e conoscenze che fanno capo alla competenza digitale e tutte concorrono a costruirla.
Competenza digitale significa padroneggiare le abilità e le tecniche di utilizzo delle nuove tecnologie, ma soprattutto utilizzarle con autonomia e responsabilità nel rispetto degli altri e sapendone prevenire ed evitare i pericoli.

In questo senso, tutti gli insegnanti e tutti gli insegnamenti sono coinvolti nella sua costruzione.

### *2.2. Piano nazionale scuola digitale*

La scuola si propone di perseguire gli obiettivi contenuti nel PNSD con le seguenti azioni:

- potenziamento degli strumenti didattici e laboratoriali necessari a migliorare la formazione e i processi di innovazione dell'istituto;
- adozione di strumenti organizzativi e tecnologici per favorire la governance, la trasparenza e la condivisione di dati, nonché lo scambio di informazioni tra ds, docenti e studenti;
- formazione dei docenti per l'innovazione didattica e sviluppo della cultura digitale per l'insegnamento, l'apprendimento e la formazione delle competenze lavorative, cognitive e sociali degli studenti;
- miglioramento delle infrastrutture di rete in tutti i plessi dell'Istituto, anche nella scuola dell'Infanzia;
- realizzazioni di Ambienti Digitali 3.0.

Anche l'adesione ai PON è un'opportunità che viene data alla Scuola per migliorare le metodologie didattiche collaborative e laboratoriali ed offrire agli allievi spazi tecnologici che permettano di sviluppare le loro conoscenze con la dovuta autonomia nella scoperta delle fonti e nella rielaborazione delle proprie conoscenze.
Questo sviluppo permetterà di ottenere una ricaduta notevole sulla didattica e sull'organizzazione scolastica (ad esempio condividere registri informatici, accedere al portale della scuola…).
Per favorire lo sviluppo della didattica digitale la scuola cercherà di arricchirsi di nuove strumentazioni digitali per la realizzazione di ambienti didattici coerenti con il Piano Nazionale.
La scuola ha aderito alle varie iniziative connesse al PNSD fra cui:

- Animatori digitali
- PON WIFI 2.0
- Scuola digitale: ambienti multimediali per attività collaborative e inclusive
- Realizzazione di smart class per la scuola del primo ciclo
- Realizzazione di reti locali, cablate e wireless, nelle scuole
- Digital board: trasformazione digitale nella didattica e nell'organizzazione
- Ambienti didattici innovativi per la scuola dell'infanzia
- Formazione del personale
- Internet day

L'istituto svolge inoltre attività di CODING ad integrazione delle competenze digitali previste dalle Indicazioni Nazionali, favorendo negli alunni lo sviluppo del "pensiero computazionale".

### *2.3. Formazione dei docenti sull'utilizzo, l'integrazione delle TIC nella didattica e sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali*

La formazione del corpo docente verrà organizzata su due livelli: interno ed esterno.
A livello interno, nel PTOF si prevede che una parte della formazione sia dedicata proprio all'uso e all'inserimento delle TIC nella didattica e ai temi informatici in generale. Buoni punti di riferimento per la formazione online sarà costituito dalle piattaforme : **"Generazioni Connesse"e la piattaforma "Elisa"** le quali forniscono diverse tipologie di corsi che analizzano il fenomeno del bullismo e cyberbullismo da diverse sfaccettature. Per quanto riguarda la formazione esterna, la scuola assicura tempestiva e capillare informazione su corsi, convegni e seminari che riguardino tali argomenti, cercando altresì di agevolare il personale che intenda parteciparvi. Infine la scuola si apre alla collaborazione con enti e associazioni locali per realizzare progetti formativi indirizzati ad alunni, docenti e genitori.

All'inizio di ogni anno scolastico la commissione Bullismo e Cyberbullismo, 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.

*2.4.Sensibilizzazione delle famiglie*

L' Istituto attiverà iniziative per sensibilizzare le famiglie sull'uso consapevole della rete.
A tal fine sono previsti momenti di incontro formativi e informativi, attuati anche con la collaborazione di associazioni e enti presenti sul territorio. Mezzo di divulgazione è il sito della scuola .
La scuola si impegna alla diffusione delle informazioni contenute nel documento di e-policy per far conoscere alle famiglie il regolamento che disciplina l'utilizzo delle nuove tecnologie, prevenendone rischi e abusi.

## 3. Gestione dell'infrastruttura e della strumentazione TIC della scuola

*3.1. Accesso ad internet: filtri antivirus e sulla navigazione*

I computer portatili collocati nelle aule accedono ad internet attraverso reti Wifi. Nei laboratori informatici sono presenti computer portatili e fissi che accedono ad internet con reti wifi e LAN. Tutti i computer presenti nella scuola hanno installato un antivirus. Gli studenti non possono accedere con il loro dispositivi alla rete internet della scuola. I docenti possono accedere con il loro dispositivi personale alla rete. Agli studenti è permesso l'accesso ad internet solo per attività didattiche con l'autorizzazione e il controllo dei docenti.

*3.2. Gestione accessi (password, backup, ecc.)*

I computer portatili presenti nella scuola non richiedono una password di accesso per l'accensione. Quelli presenti nell'aula informatica dispongono di un solo account. L'accesso ad internet è soggetto a filtri di sicurezza che impediscono la navigazione a siti di pornografia, acquisti on line, Facebook…

*3.3. E-mail*

Ogni docente possiede un account personale che ha comunicato alla scuola e che viene utilizzato per l'invio di comunicazioni e documentazioni.

*3.4. Blog e sito web della scuola*

Il sito della scuola( https://iscgaribaldi.edu.it/) è gestito dal docente responsabile piattaforma Google Space For Education.

*3.5. Registro elettronico "Mastercom Pro" e "Nuvola*

Il registro elettronico della scuola viene utilizzato anche per le comunicazioni Scuola-famiglia-docenti.

## 4. Strumentazione personale

*4.1. Utilizzo attrezzature scientifico-tecnologiche, laboratori e sussidi didattici (capo v regolamento d'istituto 2017/18)*

4.1.1 *Uso dei laboratori e aule speciali*

- I laboratori e le aule speciali sono assegnati dal Dirigente Scolastico all'inizio di ogni anno alla responsabilità di alcuni docenti che hanno il compito di mantenere una lista del materiale disponibile, tenere i registri del laboratorio, curare il calendario d'accesso allo stesso, proporre interventi di manutenzione, ripristino, sostituzione di attrezzature, ecc...
- Il responsabile di laboratorio concorda con i docenti interessati i tempi di utilizzo da parte delle classi e con il Dirigente Scolastico le modalità ed i criteri per l'utilizzo del laboratorio in attività extrascolastiche.

- Le responsabilità inerenti all'uso dei laboratori e delle aule speciali, sia per quanto riguarda la fase di preparazione delle attività sia per quella di realizzazione delle stesse con gli allievi, competono all'insegnante nei limiti della sua funzione di sorveglianza ed assistenza agli alunni.
- I laboratori e le aule speciali devono essere lasciate in perfetto ordine. Al fine di un sicuro controllo del materiale, l'insegnante prenderà nota della postazione e degli strumenti assegnati allo studente o al gruppo di studenti.
- L'insegnante avrà cura, all'inizio ed alla fine di ogni lezione, di verificare l'integrità di ogni singola postazione e di ogni singolo strumento utilizzato. L'insegnante, qualora alla fine della lezione dovesse rilevare danni che non erano presenti all'inizio, è tenuto a darne tempestiva comunicazione al responsabile di laboratorio che ne informerà il Dirigente Scolastico.

### *4.2. Utilizzo dei laboratorio d' informatica*

- Gli studenti della scuola potranno accedere al laboratorio solo se accompagnati da un docente. È espressamente vietata la permanenza in laboratorio degli alunni in assenza dell'insegnante.
- L'accesso è garantito a tutte le classi, la precedenza viene riservata agli insegnanti di "Tecnologia" secondo il calendario affisso all'interno dell'aula informatica.

#### 4.2.1 *L'utilizzo dei personal computer e delle attrezzature*

Norme generali di comportamento:

- Ogni docente dovrà compilare dettagliatamente e in ogni parte il registro del laboratorio d'informatica da richiedere al responsabile di laboratorio;
- All'accensione dei computer ogni insegnante è tenuto a procedere all'iniziale verifica dell'integrità dei sistemi; se vengono riscontrate anomalie del sistema comunicare il tutto al responsabile o alla segreteria;
- In laboratorio non è consentito consumare pasti di alcun tipo. Nell'eventualità della coincidenza con la ricreazione, gli alunni sono obbligati a uscire dall'aula computer, consumare la propria merenda e rientrare a ricreazione ultimata;
- Gli alunni sono tenuti a rispettare le consegne dell'insegnante sull'utilizzo dei computer e possono accedere al solo account "Alunno";
- Il docente che vuole conoscere l'account amministratore per l'installazione dei programmi può chiedere al responsabile di laboratorio;
- Ogni utente è personalmente responsabile dei file e dei processi della propria sessione di lavoro;
- Gli utenti sono tenuti a garantire il corretto utilizzo delle apparecchiature e ad usarle in modo da evitare qualsiasi danneggiamento hardware e software.
  In casi particolarmente gravi potranno essere ritenuti responsabili di eventuali danneggiamenti delle attrezzature;
- E' severamente vietato staccare cavi elettrici da ciabatte e prese così come i cavi di connessione alle periferiche;
- Nell'aula non è consentito il deposito di zaini e cappotti;
- All'uscita del laboratorio è cura del docente e degli alunni di risistemare tastiere, mouse, sedie e quant'altro come sono stati trovati all'ingresso e accertarsi che non si lasci nessun computer acceso compreso monitor, casse acustiche, stampanti, scanner...
- Per comunicazioni di malfunzionamento dei sistemi e quant'altro non contemplato in questo regolamento contattare il responsabile del laboratorio.

#### *4.2.2. Uso di internet*

- La ricerca su internet e l'uso della posta elettronica sono destinate alle finalità didattiche, scolastiche e di aggiornamento.
- Gli alunni possono navigare su internet solo sotto la diretta sorveglianza del docente; il docente non solo è tenuto a verificare continuamente la navigazione ma è *anch*e direttamente responsabile dell'utilizzo di internet da parte degli alunni cui ha dato la possibilità di collegarsi alla rete. Al termine della sessione gli utenti avranno cura di disconnettersi da internet.
- È compito dei docenti accompagnatori controllare i materiali scaricati dagli alunni durante la navigazione.

*4.2.3. Utilizzo delle stampanti*

- La stampa di documenti da parte degli alunni deve avvenire dietro esplicita autorizzazione del docente.
- Il permesso per la stampa di un numero elevato di pagine o di lavori che prevedono un consumo particolarmente oneroso di inchiostro e carta, va richiesto agli uffici di segreteria. In tal caso va previsto l'acquisto del consumabile idoneo all'interno dei piano finanziario del progetto.

*4.2.4. Utilizzo del tablet per la gestione del registro elettronico*

- Il docente della prima ora è tenuto a portare nella propria classe il tablet custodito in presidenza ma che al mattino i collaboratori scolastici addetti hanno il compito di posizionarli in corridoio. Durante lo svolgimento delle attività, il docente può utilizzare il tablet per accedere al registro elettronico e compilare le parti del registro di classe. Al cambio dell'ora ogni docente dovrà assicurarsi che il tablet sia sotto custodia dell'insegnante dell'ora successiva, che lo utilizzerà secondo le modalità indicate al punto precedente.
- Durante l'intervallo i docenti avranno particolare cura nella custodia personale dei tablet. Al termine dell'intervallo saranno consegnati in classe al docente in servizio nell'ora successiva.
- L'insegnante dell'ultima ora è tenuto a riportare il tablet nell'apposito carrello riservato alla custodia dello strumento, provvedendo a metterlo in carica nelle prese già predisposte.
- I tablet che dovessero presentare anomalie durante la mattinata sono invece riposti a parte, in uno spazio predisposto che ogni scuola avrà individuato, per poter essere controllato dall'incaricato a tale scopo.
- Qualsiasi malfunzionamento e/o segnalazione dovrà pervenire esclusivamente per iscritto al responsabile del plesso che informerà la dirigenza della questione.
- Al termine della giornata, nel caso in cui i tablet si trovino in un'aula non protetta, sarà cura del collaboratore scolastico addetto di riporli nello spazio destinato con chiusura a chiave.
- Gli insegnanti supplenti temporanei riceveranno, per il periodo limitato alla sostituzione del titolare assente, apposite credenziali di accesso al registro elettronico dall'ufficio di segreteria.

Si ricorda a tutto il personale che lo strumento assegnato ad ogni classe deve essere utilizzato prevalentemente per la compilazione del registro elettronico. Può essere possibile altro utilizzo a scopo didattico tenendo in considerazione che non è consentito:

- alterare le configurazioni del desktop;
- installare applicazioni senza autorizzazione;
- modificare e/o cancellare programmi;
- inserire password aggiuntive per sbloccare o disabilitare qualsiasi funzione o documento;
- utilizzare l'applicazione della fotocamera e dei registratori audio/video per non incorrere a gravi violazioni della privacy ;
- utilizzare la rete per attività personali e non di docenza.

*4.2.5 Utilizzo di smartphone e tablet*

I docenti e gli alunni:

- possono utilizzare smartphone e tablet per riprendere le attività didattiche, a corredo della documentazione, se previsto dalla progettazione didattica, per l'uso del libro digitale o specifiche applicazioni.
- non possono utilizzare il proprio smartphone e/o tablet, per fare foto e video o per diffondere immagini ai fini esclusivamente personali.

## 5. Prevenzione, rilevazione e gestione dei casi

Le misure di prevenzione comprendono l'integrazione nel curricolo dei temi legati al corretto utilizzo delle TIC e di Internet: la progettazione di unità formative specifiche deve essere pianificata a livello di dipartimenti disciplinari, garantendo un intervento su ogni classe, anche con docenti non titolari della classe.

La scuola si avvale della collaborazione di enti e associazioni per realizzare incontri rivolti alla componente studentesca e alle famiglie con l'intento di fornire ogni elemento utile alla prevenzione e alla gestione dei problemi relativi alla sicurezza informatica; gli interventi che sono pianificati, anche all'interno di percorsi specifici, promossi e attivati nei laboratori PON.
La rilevazione dei casi è compito dell'intera comunità educante, secondo la sensibilità di ciascuno e la presenza in particolari momenti o contesti.

Gli insegnanti, per la natura stessa del loro lavoro, devono in molti casi fungere da "torre di avvistamento", avamposto privilegiato delle problematiche e dei rischi che bambini e adolescenti possono trovarsi ad affrontare ogni giorno.
Responsabilità degli insegnanti è, dunque, imparare a riconoscere i rischi più comuni che i ragazzi possono correre sul web, per potere poi intervenire adeguatamente. Tra questi, un'attenzione specifica andrà prestata ai fenomeni di:

- bullismo/cyberbullismo – una forma di prepotenza virtuale e non, attuata attraverso l'uso di internet e delle tecnologie digitali;
- sexting - pratica di inviare o postare messaggi di testo e immagini a sfondo sessuale, come foto di nudo o semi-nudo, via cellulare o tramite Internet;
- adescamento o grooming – una tecnica di manipolazione psicologica, che gli adulti potenziali abusanti utilizzano online, per indurre i bambini/e, adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata;

I rischi che gli alunni possono correre a scuola derivano da un uso non corretto dei dispositivi elettronici, in particolare di quelli personali.

*5.1. Prevenzione*

Tra le azioni utili a contrastare i rischi derivanti da un utilizzo improprio dei dispositivi digitali da parte degli studenti vi sono le seguenti:

- Diffondere un'informazione capillare rivolta al personale scolastico, agli studenti e alle famiglie, sui rischi che i minori possono correre sul web, attraverso la creazione di un'apposita area sul sito della scuola dedicata alla sicurezza in rete;
- Organizzare incontri tenuti da psicologi nelle singole classi aventi per oggetto le tematiche del cyberbullismo, del sexting e dell'adescamento;
- Richiedere 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);
- Non consentire l'utilizzo del cellulare personale degli alunni a scuola, in quanto per assolvere a comunicazioni urgenti con i genitori o con chi ne fa le veci è sempre disponibile il telefono della scuola supervisionato dal personale addetto al centralino, che prima di passare la telefonata si accerta dell'identità dell'interlocutore.
- Consentire l'utilizzo del cellulare sono in casi particolari ed eccezionali, ad esempio quando ci si trova fuori dal contesto scolastico durante una visita guidata, e comunque sotto la supervisione dell'insegnante, che si accerta preventivamente dell'identità dell'interlocutore.
- Utilizzare filtri e software che impediscano il collegamento a siti web per adulti (black list).
- Attento monitoraggio da parte del personale docente affinché il presente regolamento venga rispettato;
- Tempestivo intervento tramite opportuna sanzione qualora il regolamento venga disatteso.

*5.2 Rilevazione*

Si considerano da segnalare tutte quelle situazioni che si configurano come episodi di cyberbullismo (caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona o un piccolo gruppo tramite un utilizzo irresponsabile dei social network), ma anche usi inappropriati della rete (siti d'odio, contenuti non adatti all'età degli alunni…).

I docenti di classe informano il referente per il bullismo/cyberbullismo. Il referente informa il Dirigente Scolastico, il quale procede ad informare le famiglie. Tutte le segnalazioni riportate dai docenti vengono registrate su apposita scheda (diario di bordo).

*5.3 Gestione dei casi*

Per un'efficace gestione dei casi, i docenti si attengono alle modalità illustrate negli schemi seguenti messi a disposizione da Generazioni Connesse .

Generazioni Connesse

Progetto co-finanziato

**5. Prevenzione, rilevazione e gestione dei casi**

***PREVENZIONE***

| Rischi: | Azioni |
|---|---|
| Alunno usa il proprio cellulare durante la lezione per comunicare con esterni, per fotografare o girare video. | Vietare l'uso del cellulare tramite regolamento scolastico<br>Controllo che venga rispettato il divieto |
| Alunno pubblica sui social networks video e foto realizzati in classe | Organizzare attività che promuovano l'uso corretto del cellulare e dei social networks, mediante anche l'intervento di esperti esterni |
| Alunno usa i pc della scuola per collegarsi a siti non consentiti e/o scaricare materiale non consentito. | Utilizzo di sistemi di controllo per la navigazione sicura<br>Educare a selezionare le informazioni reperibili in rete |

# Schema riepilogativo delle situazioni gestite legate a rischi online

## Diario di bordo

| NOME | DATA | ORA | EPISODIO | AZIONI INTRAPRESE | | INS. CON CUI L'ALUNNO/A SI E' CONFIDATO | FIRMA |
|---|---|---|---|---|---|---|---|
| | | | | COSA | DA CHI ? | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

## *RILEVAZIONE E GESTIONE DEI CASI*

| Che cosa segnalare | Come segnalare: quali strumenti e a chi. | Come gestire le segnalazioni | Definizione delle azioni da intraprendere a seconda della specifica del caso. |
|---|---|---|---|
| L'uso di cellulari in orario scolastico<br>Uso del pc per scaricare o visualizzare materiale non consentito | Si segnala verbalmente al Dirigente e alla famiglia | Informativa agli alunni e alle famiglie sulle norme che regolano la diffusione di immagini e dati personali e sulle sanzioni che la norma prevede. | Il cellulare viene requisito, il genitore è tenuto ad andare a ritirarlo. |
| Uso di cellulare per riprendere senza autorizzazione scene di vita scolastica | Si segnala al Dirigente e per iscritto alla famiglia | | Il cellulare viene requisito, il genitore è tenuto ad andare a ritirarlo.<br>Si chiede la cancellazione delle immagini ed eventualmente l'eliminazione di quelle pubblicate. |
| Uso di cellulare per compiere atti di cyberbullismo | Si segnala al Dirigente e per iscritto alla famiglia e alle agenzie di controllo | | |



## 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? | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

**MODULO PER LA SEGNALAZIONE DI CASI**

Nome di chi compila la segnalazione: Ruolo:

Data: Scuola:

| | |
|---|---|
| Descrizione dell'episodio o del problema | |
| Soggetti coinvolti | Vittima/e: Classe:<br>1.<br>2.<br>3.<br>Bullo/i:<br>1.<br>2.<br>3.<br>Classe: |
| Chi ha riferito dell'episodio? | - La vittima<br>- Un compagno della vittima, nome:<br>- Genitore, nome:<br>- Insegnante, nome:<br>- Altri, specificare: |
| Atteggiamento del gruppo | Da quanti compagni è sostenuto il bullo?<br><br>Quanti compagni supportano la vittima o potrebbero farlo? |
| Gli insegnanti sono intervenuti in qualche modo ? | |
| La famiglia o altri adulti hanno cercato di intervenire ? | |
| Chi è stato informato della situazione? | □ coordinatore di classe data:<br>□ consiglio di classe data:<br>□ dirigente scolastico data:<br>□ la famiglia della vittima/e data:<br>□ la famiglia del bullo/i data:<br>□ le forze dell'ordine data:<br>□ altro, specificare: |

**MODULO PER IL FOLLOW-UP DEI CASI**

| | AZIONI INTRAPRESE | La situazione è |
|---|---|---|
| Aggiornamento 1 | | □ migliorata □ invariata □ peggiorata<br>Come: |
| Aggiornamento 2 | | □ migliorata □ invariata □ peggiorata<br>Come: |
| Aggiornamento 3 | | □ migliorata □ invariata □ peggiorata<br>Come: |
| | | |
| | | |

*6. Annessi*

## *6. 1* PROCEDURE OPERATIVE PER LA RILEVAZIONE, IL MONITORAGGIO E LA GESTIONE DELLE SEGNALAZIONI.

**CYBERBULLISMO: alcuni campanelli di allarme.**
Gli atti di bullismo avvengono prevalentemente entro o nei dintorni del contesto scolastico; tuttavia, sempre più in misura crescente le prepotenze vengono riportate nel contesto virtuale di Internet. In queste situazioni si parla di *Cyberbullying* che si manifesta attraverso:

- invio di sms, mms, e-mail offensivi/o di minaccia;
- diffusione di messaggi offensivi ai danni della vittima, attraverso la divulgazione di sms o e-mail nelle mailing-list o nelle chat-line;
- pubblicazione nel cyberspazio di foto o filmati che ritraggono prepotenze o in cui la vittima viene denigrata.

La rilevazione diretta degli indicatori da parte degli insegnanti o indiretta, sulla base di quanto riferito dagli alunni o dai genitori, deve affinarsi con l'osservazione delle relazioni interpersonali e delle possibili dinamiche conflittuali sottostanti presenti nel contesto classe, al fine di verificare l'entità e la natura del fenomeno e dare avvio al programma di intervento.

**A chi segnalare:**
L'attuazione del programma di intervento si basa prevalentemente sull'impiego delle risorse umane già presenti e disponibili: docenti e altro personale scolastico, alunni e genitori. Non serve, se non in casi particolarmente gravi, l'opera di psicologi, assistenti sociali, o altri specialisti. L'elemento fondamentale per una buona riuscita del programma è infatti la corretta ristrutturazione del contesto relazionale degli alunni.
Non operare in modo isolato, ma confrontarsi con i colleghi di classe e il Dirigente Scolastico.

Se subisci ricatti o diffusione di foto e messaggi privati rivolgiti agli operatori del Servizio di helpline facendo il numero telefonico 1.96.96 gestito da Telefono Azzurro nell'ambito del progetto Generazioni Connesse. Gli operatori sono disponibili ad offrirti uno spazio confidenziale di ascolto e di aiuto anche attraverso la chat presente sul sito www.azzurro.it/chat. Il servizio telefonico è attivo 24 ore su 24; la chat è invece operativa tutti i giorni dalle 8 alle 22, il sabato e domenica fino alle 20.

Siti Web dai contenuti illeciti o contatti con persone sospette devono essere segnalati alla Polizia Postale e delle Comunicazioni all'indirizzo: www.commissariatodips.it

Il 114 è il numero di emergenza al quale rivolgersi tutte le volte che un bambino è in pericolo; è attivo 24 ore su 24, sette giorni su sette, è gratuito ed è raggiungibile sia dal telefono di casa che dal telefono mobile. Il sito www.114.it consente di accedere a materiali utili in caso di violenza di qualsiasi tipo sui minori; è possibile anche accedere alle FAQ.

Se qualcuno riceve insulti dal tuo profilo Facebook (e tu non sei l'artefice dei messaggi) vuol dire che sono riusciti a scoprire la password di accesso al suo account. Devi chiamare 19696 e farti aiutare ad impostare correttamente la privacy in Facebook e formulare una nuova password che ti consenta di mantenere privati i dati personali. Ogni abuso subito o rilevato nella navigazione, deve essere segnalato tramite i canali e gli strumenti offerti dal servizio. Devi parlarne con i genitori affinché segnalino l'accaduto alla Polizia Postale.

**PROCEDURE OPERATIVE PER LA GESTIONE DEI CASI.**

**LINEE GUIDA PER ALUNNI**

1) Non comunicare mai a nessuno la tua password e periodicamente cambiala, usando numeri, lettere e caratteri speciali.
2) Mantieni segreto il nome, l'indirizzo, il telefono di casa, il nome e l'indirizzo della tua scuola.
3) Non inviare a nessuno fotografie tue o di tuoi amici.
4) Prima di inviare o pubblicare su un Blog la fotografia di qualcuno, chiedi sempre il permesso.
5) Chiedi sempre al tuo insegnante a scuola o ai tuoi genitori a casa il permesso di scaricare documenti dalla Rete.
6) Chiedi sempre il permesso prima di iscriverti a qualche concorso o prima di riferire l'indirizzo della tua scuola.
7) Quando sei connesso alla rete RISPETTA SEMPRE GLI ALTRI, ciò che per te è un gioco può rivelarsi offensivo per qualcun altro.
8) Non rispondere alle offese ed agli insulti.
9) BLOCCA I BULLI: molti Blog e siti Social Network ti permettono di segnalare i *cyberbulli*.
10) Conserva le comunicazioni offensive, ti potrebbero essere utili per dimostrare quanto ti è accaduto.
11) Se ricevi materiale offensivo (email, sms, mms, video, foto, messaggi vocali) non diffonderlo: potresti essere accusato di *cyberbullismo*.
12) Rifletti prima di inviare: ricordati che tutto ci che invii su Internet diviene pubblico e rimane PER SEMPRE.
13) Riferisci al tuo insegnante o ai tuoi genitori se qualcuno ti invia immagini che ti infastidiscono e non rispondere; riferisci anche al tuo insegnante o ai tuoi genitori se ti capita di trovare immagini di questo tipo su Internet.
14) Se qualcuno su Internet ti chiede un incontro di persona, riferiscilo al tuo insegnante o ai tuoi genitori.
15) Ricordati che le persone che incontri nella Rete sono degli estranei e non sempre sono quello che dicono di essere.
16) Non è consigliabile inviare mail personali, perciò rivolgiti sempre al tuo insegnante o ai tuoi genitori prima di inviare messaggi.
17) Non scaricare (*download*) o copiare materiale da Internet senza il permesso del tuo insegnante o dei tuoi genitori.
18) Non caricare (*upload*) materiale video o fotografico nei siti web dedicati senza il permesso del tuo insegnante o dei tuoi genitori.

**LINEE GUIDA PER INSEGNANTI**

1) Evitate di lasciare le e-mail o file personali sui computer o sul server della scuola, lo spazio è limitato e di uso comune.
2) Salvate sempre i vostri lavori (file) in cartelle personali e/o di classe e non sul desktop o nella cartella del programma in uso. Sarà cura di chi mantiene il corretto funzionamento delle macchine cancellare file di lavoro sparsi per la macchina e al di fuori delle cartelle personali.
3) Discutete con gli alunni della e-Safety Policy della scuola, di utilizzo consentito della Rete, e degli eventuali problemi che possono verificarsi nell'applicazione delle regole relative all'uso di Internet.
4) Date chiare indicazioni su come si utilizza Internet, ed eventualmente anche la posta elettronica e informate gli alunni che le navigazioni saranno monitorate.
5) Ricordate di chiudere la connessione (e di spegnere il computer) alla fine della sessione di lavoro su Internet e disabilitare la navigazione in Rete del Laboratorio (qualora sia stata attivata).
6) Ricordate agli alunni che la violazione consapevole della e-Safety Policy della scuola comporta sanzioni di diverso tipo.
7) Adottate provvedimenti disciplinari, proporzionati all'età e alla gravità del comportamento.
8) Adottate interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi, di ridefinizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli alunni della classe, di prevenzione e gestione positiva dei conflitti, di moderazione dell'eccessiva competitività, di promozione di rapporti amicali e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni.
9) Nelle situazioni psico-socio-educative particolarmente problematiche, convocate i genitori (o gli esercenti la potestà) per valutare con loro a quali risorse territoriali possono rivolgersi: sportello di ascolto

psicologico, Servizi Sociali per la fruizione di servizi socio-educativi comunali, ASL per quanto di competenza psicologica e psicoterapeutica (Pediatria, Neuropsichiatria infantile, Consultorio Familiare).

10) Chiedete/suggerite di cancellare il materiale offensivo, bloccare o ignorare particolari mittenti, uscire da gruppi non idonei, cambiare indirizzo e-mail, ecc.
11) Segnalate la presenza di materiale pedopornografico (senza scaricarlo o riprodurlo) alla Polizia Postale o al Telefono Azzurro.
12) In caso di abuso sessuale rilevato anche attraverso i nuovi mezzi di comunicazione come Internet o il cellulare, confrontatevi con i colleghi di classe e il Dirigente Scolastico, denunciate all'autorità giudiziaria o agli organi di Polizia.

**CONSIGLI AI GENITORI PER UN USO RESPONSABILE DI INTERNET A CASA**

**Consigli generali**

1) Posizionate il computer in salone o in una stanza accessibile a tutta la famiglia.
2) Evitate di lasciare le e-mail o file personali sui computer di uso comune.
3) Concordate con vostro figlio le regole: quando si può usare Internet e per quanto tempo.
4) Inserite nel computer i filtri di protezione: prevenire lo *spam*, i *pop-up* pubblicitari, l'accesso a siti pornografici.
5) Aumentate il filtro del *parental control* attraverso la sezione sicurezza in Internet dal pannello di controllo.
6) Attivate il *firewall* (protezione contro *malware)* e antivirus.
7) Mostratevi coinvolti: chiedete a vostro figlio di mostrarvi come funziona Internet e come viene usato per scaricare e caricare compiti, lezioni, materiali didattici e per comunicare con l'insegnante.
8) Incoraggiate le attività online di alta qualità: ricercare informazioni scientifiche, ricercare nuovi *amici* nel mondo.
9) Partecipate alle esperienze online: navigate insieme a vostro figlio, incontrate amici online, discutete gli eventuali problemi che si presentano.
10) Comunicate elettronicamente con vostro figlio: inviate, frequentemente, e-mail, Instant Message.
11) Spiegate a vostro figlio che la password per accedere ad alcune piattaforme è strettamente personale e non deve essere mai fornita ai compagni o ad altre persone.
12) Stabilite ci che ritenete inaccettabile (razzismo, violenza, linguaggio volgare, pornografia).
13) Discutete sul tema dello scaricare file e della possibilità di ricevere file con virus.
14) Raccomandate di non scaricare file da siti sconosciuti.
15) Incoraggiate vostro figlio a dirvi se vedono immagini particolari o se ricevono e-mail indesiderate.
16) Discutete nei dettagli le conseguenze che potranno esserci se vostro figlio visita deliberatamente siti non adatti, ma non rimproveratelo se compie azioni involontarie.
17) Spiegate a vostro figlio che le *password*, i codici *pin*, i numeri di carta di credito e i numeri di telefono e i dettagli degli indirizzi e-mail sono privati e non devono essere dati ad alcuno.
18) Spiegate a vostro figlio che non tutti in Internet sono chi realmente dichiarano di essere; di conseguenza i vostri ragazzi non dovrebbero mai accordarsi per appuntamenti senza consultarvi prima.
19) Il modo migliore per proteggere vostro figlio è usare Internet con loro, discutere e riconoscere insieme i rischi potenziali.

**Consigli in base all'età**

**Se vostro figlio ha meno di 8 anni:**

- Selezionate con molta attenzione i siti *sicuri*: ricordate che i gestori dei siti, per trarre il massimo guadagno, permettono agli inserzionisti di pubblicizzare i propri prodotti;
- Comunicate a vostro figlio tre semplici regole:
- non dare il tuo vero nome, indirizzo e numero di telefono. Usa sempre il tuo *username* o *nickname*;
- se compare sullo schermo qualche messaggio o *banner*, chiudilo: insegna a tuo figlio come si fa;
- naviga esclusivamente sui siti autorizzati dai genitori: se vuoi andare su un nuovo sito, dobbiamo andarci INSIEME (molti siti richiedono la registrazione. Insegna a tuo figlio come registrarsi senza rivelare informazioni personali).

**Se vostro figlio ha tra gli 8 anni e i 10 anni**

- Progressivamente diminuite la supervisione: dagli otto ai dieci anni permettete a vostro figlio di navigare da solo nei siti autorizzati, sottolineando che deve consultarvi prima di esplorare dei nuovi.
- Verificate periodicamente i contenuti dei siti *sicuri*.
- Discutete con vostro figlio i rischi che possono presentarsi durante la navigazione on line; controllate, dalla *Cronologia* il menu navigazione, se vostro figlio ha consultato siti non autorizzati per i quali non vi ha chiesto il permesso.
- Supervisionate l'email di vostro figlio dopo averlo reso consapevole del fatto che avete pieno accesso alle sue comunicazioni.
- Se vostro figlio vuole usare Instant Messaging (IM) verificate che i suoi contatti siano limitati agli amici conosciuti.
- Specificate che non può inserire nuovi contatti senza avervi prima consultato.
- Comunicate che è assolutamente vietato cliccare su un link, contenuto in una email, su un *pop-up* pubblicitario o su un *banner* (ricordati, infatti, che potrebbero presentarsi immagini pornografiche o che potrebbe avviarsi il download di *malware*).
- Incoraggiare l'uso di Internet per svolgere ricerche scolastiche.

Definite il tempo massimo di connessione ed incoraggiate le attività con il mondo reale

**Se vostro figlio ha tra gli 11 anni e i 13 anni**

Vostro figlio è diventato grande e potrebbe dirvi che il suo migliore amico ha la possibilità di navigare tutti i giorni a tutte le ore. Che fare?

- Create una *partnership* con i genitori dei migliori amici di tuo figlio in modo da concordare con loro le regole: tempi di connessione, fasce orarie, siti autorizzati, modalità di utilizzo di IM.
- Aiutate vostro figlio a creare una rete on line sicura: siti controllati ed amici conosciuti.

**Se vostro figlio ha oltre 13 anni**

- Verificate i profili di vostro figlio e dei suoi amici, nei siti cerca persona, informandolo dei vostri periodici controlli. Ricordatevi che in questa fascia di età aumentano le ricerche di materiale sessuale ed i rischi di seduzioni sessuali on line da parte di *cyberpredatori* adulti: condividete con vostro figlio le procedure per navigare in sicurezza ed evitate *on line* ed *off line* brutti incontri.
- Confrontatevi con vostro figlio su tutti questi rischi e se protesta per il controllo, ribadite che è un dovere del genitore supervisionare e monitorare l'uso di Internet.
- Stringete un accordo: se vostro figlio dimostra di avere compreso i rischi e di sapere e volere usare Internet in modo sicuro, diminuite la supervisione.
- Il computer deve rimanere in salone o in una stanza accessibile a tutta la famiglia e non nella camera di vostro figlio ALMENO fino ai 16 anni.

## 6.2 PROTOCOLLI SIGLATI CON LE FORZE DELL'ORDINE E I SERVIZI DEL TERRITORIO PER LA GESTIONE CONDIVISA DEI CASI.

Forme ricorrenti di collaborazione nella prevenzione e contrasto del *bullismo* e del *cyberbullismo tra la Dirigente scolastica e* l'Ente Locale, del Comando dei Carabinieri, della Polizia Postale e di associazioni.

Approvato dal Collegio dei docenti in data con delibera n.

SCHEDA

COME ACCORGERTI SE UN TUO/A ALUNNO/A È COINVOLTO IN EPISODI DI CYBERBULLISMO/

In questa scheda puoi trovare alcuni indicatori (sotto forma di domande-stimolo e/o consigli) per verificare se nella tua classe ci possono essere episodi di cyberbullismo/bullismo. Ricorda che è più facile accorgersi di episodi di bullismo, che possono avvenire anche sotto il tuo sguardo, piuttosto che di cyberbullismo, dove le prevaricazioni vengono perpetrate nei luoghi virtuali in cui bambini e adolescenti si ritrovano (in particolare i social). Ricorda infine che l'elenco non è esaustivo di ciò che puoi osservare (la realtà è sempre più complessa di come la si può descrivere); gli indicatori sono segnali ai quali dovresti prestare attenzione ma che non hanno la pretesa di identificare in modo assoluto una situazione di cyberbullismo, soprattutto se considerati isolatamente.

a) Se hai il dubbio che un tuo alunno/a possa essere preso di mira da cyberbulli, ti invitiamo a riflettere sulle seguenti domande/stimolo.

1) Hai alunni che mostrano segnali di tensione o nervosismo quando ricevono messaggi sullo smartphone?

2) Hai alunni che nascondono lo smartphone in tua presenza o che ti sembrano timorosi o preoccupati di farsi vedere connessi?

3) Hai alunni che ti sembrano timorosi o preoccupati di accedere ai propri contenuti online (come ad esempio la casella mail o profili sui social) in tua presenza?

4) Hai alunni che presentano comportamenti / abitudini che causano irritazione in compagni e adulti (che, ad esempio, vengono isolati online dai compagni)?

5) Hai alunni che non sono inseriti o sono stati esclusi dai gruppi dei servizi di messaggistica istantanea (Whatsapp, telegram, viber, etc.) o social della classe?

b) Se hai il dubbio che un tuo alunno/a possa essere preso di mira da bulli, ti invitiamo a riflettere sulle seguenti domande/stimolo.

1) Hai alunni che passano molto tempo da soli (per esempio durante gli intervalli o le ore di Educazione Fisica), che vengono sistematicamente esclusi dal gruppo-classe (non hanno amici nel gruppo classe, vengono scelti per ultimi nei lavori di gruppo) o che ricercano la vicinanza degli adulti anche nei momenti di intervallo preferendo parlare con un insegnante o un operatore scolastico o stare soli piuttosto che nel gruppo dei pari?

2) Hai alunni che sono diventati più insicuri e spaventati quando parlano in classe davanti ai compagni? Hai notato o sai che questo stesso comportamento non l'hanno in altri contesti o quando devono parlare a degli adulti? Non era mai accaduto prima?

3) Hai alunni che hai sempre reputato bravi e che invece da qualche tempo a questa parte hanno avuto un calo nel rendimento scolastico per il quale non riesci a comprenderne le cause? o che subiscono ripetutamente il furto, il danneggiamento e la dispersione di oggetti o beni materiali (libri, merenda, denaro…)?

4) Hai alunni che nell'ultimo periodo mostrano cambiamenti nei comportamenti, in particolare si sono chiusi in se stessi, parlano meno con i compagni di classe e sembrano in costante stato di allerta e paura? o che reagiscono in modo impulsivo o aggressivo a quelle che a tuo avviso sono battute o scherzi tra compagni?

5) Hai alunni che nell'ultimo periodo hanno fatto assenze frequenti senza che i colloqui con i genitori ti abbiano aiutato a scoprirne le cause?

Ricorda che, nei casi più estremi il bambino o l'adolescente preso di mira dai compagni potrebbe arrivare a provocarsi ferite volontariamente o minacciare fughe o esplicitare il desiderio di togliersi la vita: tutti questi segnali denotano un malessere che, anche se non esplicitato in modo diretto, è sintomo di una causa da ricercare.

c) Se pensi che qualche alunno/a possa essere bullo o cyberbullo, ti invitiamo a riflettere sulle seguenti domande/stimolo:

1) Hai alunni con la tendenza a prendere in giro sempre le stesse persone, anche attraverso post online o foto o messaggi vocali di cui altri alunni si lamentano?

2) Hai alunni che mostrano una tendenza costante ad avere comportamenti prevaricatori o di comando nei riguardi dei compagni? o che nei social o nel gruppo whatsapp della classe "governano" le conversazioni?

3) Hai alunni che faticano ad essere empatici nei confronti di qualche compagno che ha subito il furto di un oggetto in classe? O che mostrano disattenzione rispetto agli stati emotivi di chi è in difficoltà? O che fatica a smettere di prendere in giro un compagno a motivo di qualcosa visto sul suo profilo online?

Se riconosci nelle situazioni descritte, anche solo in parte, ciò che accade nella tua classe, può esserti utile approfondire la situazione sia coinvolgendo la classe che la comunità scolastica o confrontandoti con esperti per capire come approfondire la situazione e offrire ai minori coinvolti, se lo desiderano, l'eventuale supporto necessario. Il cyberbullismo è un fenomeno relazionale e per contrastarlo ed affrontarlo occorre l'impegno di tutti.