



**MINISTERO DELL'ISTRUZIONE**  
**UFFICIO SCOLASTICO REGIONALE PER IL LAZIO**  
**Istituto d'Istruzione Superiore "Margherita HACK"**  
**Largo Giovanni Paolo II, 1 – 00067 Morlupo (RM)**  
**Cod. Mec. RMIS093003 - Cod. Fisc. 97197630581**  
 Tel. 06/99180813 - Fax 06/9071935 - Distr. 31

Sede legale: Liceo Scientifico-Linguistico-Scienze Umane "Giuseppe Piazzi" Morlupo (RM) Cod. Mec. RMPS09301D

Sez. associata: I.T.C.G. "P.L. Nervi" Rignano Flaminio (RM) Cod. Mec. RMTD093019

Sez. associata: I.P.S.C.T. "P.L. Nervi" Rignano Flaminio (RM) Cod. Mec. RMRC093012

Sez. associata: I.T.C.G. "P.L. Nervi" serale Rignano Flaminio (RM) Cod. Mec. RMTD09351P

E-mail: [rmis093003@istruzione.it](mailto:rmis093003@istruzione.it)

PEC: [rmis093003@pec.istruzione.it](mailto:rmis093003@pec.istruzione.it)

Sito web: [www.iismargheritahack.edu.it](http://www.iismargheritahack.edu.it)

## E-Safety

## Policy

**A.S. 2021/2022 – 2023/2024**

Approvato con delibera

n. 15 del Collegio dei docenti del 22/10/2021

n. xx del Consiglio d'Istituto del xx-xx-xxxx



# INDICE

## **1. Introduzione**

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

## **2. Formazione e Curricolo**

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

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

- 3.1 Accesso ad internet: filtri, antivirus e sulla navigazione.
- 3.2 Gestione accessi (password, backup, ecc.).
- 3.3 E-mail.
- 3.4 Blog e sito web della scuola.
- 3.5 Social network.
- 3.6 Protezione dei dati personali.

## **4. Strumentazione personale**

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

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

### **5.1 *Prevenzione***

- 5.1.1 Rischi
- 5.1.2 Azioni

### **5.2 *Rilevazione***

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

### **5.3 *Gestione dei casi***

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

# 1. Introduzione

## 1.1 Scopo della e-Safety Policy

Scopo del presente documento è quello di informare l'utenza per un uso corretto e responsabile delle apparecchiature informatiche collegate alla rete in dotazione alla Scuola, nel rispetto della normativa vigente.

La scuola si impegna pertanto a promuovere un uso positivo e responsabile delle Tecnologie dell'Informazione e della comunicazione (TIC) garantendo anche un sistema per il monitoraggio e il controllo della sicurezza on-line. Gli studenti acquisiranno (matureranno) non solo procedure e competenze "tecniche", ma anche corrette norme comportamentali al fine di prevenire le problematiche che derivano da un utilizzo non responsabile e pericoloso (dannoso) delle tecnologie digitali a scuola. Vuol dire sviluppare negli alunni la *competenza digitale* ritenuta dall'Unione Europea competenza chiave per la sua importanza e pervasività nel mondo d'oggi.

I Nuovi Media sono entrati a far parte della vita della maggior parte dei pre-adolescenti e adolescenti italiani, supportando e facilitando la comunicazione e, potenzialmente, la collaborazione. Rappresentano uno strumento di espressione e partecipazione che influenza la società e la vita personale degli individui di ogni età, ma in particolare dei più giovani.

Gli studenti devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete. Di fatto esiste la possibilità che durante il lavoro online si possa entrare accidentalmente in contatto con materiale inadeguato e/o illegale, pertanto la Scuola promuove l'adozione di strategie che limitino l'accesso a siti e/o applicazioni illeciti.

In questo contesto, gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di indicare regole di condotta chiare per un uso critico e consapevole di Internet anche a casa, per prevenire il verificarsi di situazioni potenzialmente pericolose.

Attraverso l'E-policy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso di Internet. L'E-policy fornisce, quindi, delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

## 1.2 Ruoli e Responsabilità

Affinché l'E-policy sia davvero uno strumento operativo efficace per la scuola e tutta la comunità educante è necessario che ognuno, secondo il proprio ruolo, s'impegni nell'attuazione e promozione di essa.

### **Ruoli e Responsabilità** *(che cosa ci si aspetta da tutti gli attori della Comunità Scolastica)*

<b>RUOLO</b>	<b>RESPONSABILITA'</b>
<b>DIRIGENTE SCOLASTICO</b>	<ul style="list-style-type: none"><li>• La responsabilità generale per i dati e la sicurezza dei dati;</li><li>• garantire che la scuola utilizzi un internet service filtrato approvato, conforme ai requisiti di legge vigenti;</li><li>• la responsabilità di assicurare che tutti gli insegnanti ricevano una formazione adeguata per svolgere i ruoli di sicurezza on-line e per la formazione di altri colleghi;</li><li>• garantire l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line;</li><li>• essere a conoscenza delle procedure da seguire in caso di infrazione della E-Safety Policy;</li><li>• 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;</li><li>• ruolo di primo piano nello stabilire e rivedere la E-Safety Policy.</li></ul>

<p>DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI</p>	<ul style="list-style-type: none"> <li>• 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;</li> <li>• 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.</li> </ul>
<p>ANIMATORE DIGITALE</p>	<ul style="list-style-type: none"> <li>• Pubblicare la E-Safety Policy sul sito della scuola;</li> <li>• garantire che tutti i dati relativi agli alunni pubblicati sul sito siano sufficientemente tutelati;</li> <li>• stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornire consulenza e informazioni al personale in relazione ai rischi on-line e alle misure di prevenzione e gestione degli stessi;</li> <li>• monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, nonché proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;</li> <li>• coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti la "scuola digitale".</li> </ul>

DOCENTI  
e figure educative che  
li affiancano

- 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;
  - comprendere e contribuire a promuovere politiche di sicurezza in internet;
  - assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;
  - segnalare qualsiasi problema o proposta di carattere tecnico-organizzativo ovvero esigenza di carattere informativo all'Animatore digitale ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC;
  - garantire che gli alunni capiscano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet;
- integrare tematiche legate alla sicurezza on-line nel curriculum di studio e nelle attività didattiche ed educative delle classi;
- assicurare che gli alunni abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore;
  - supervisionare e guidare gli alunni con cura quando sono impegnati in attività di apprendimento che coinvolgono la tecnologia on-line e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;
  - 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;

	<ul style="list-style-type: none"> <li>• comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;</li> <li>• segnalare al Dirigente scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dalle norme.</li> </ul>
ALUNNI	<ul style="list-style-type: none"> <li>• 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;</li> <li>• Essere informati, comprendere e accettare la E-Safety Policy;</li> <li>• 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;</li> <li>• esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori.</li> <li>• comprendere l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi;</li> <li>• adottare condotte rispettose degli altri anche quando si comunica in rete;</li> <li>• capire l'importanza di segnalare abusi, l'uso improprio o l'accesso a materiali inappropriati;</li> <li>• sapere quali azioni intraprendere se loro o qualcuno che conoscono si sente preoccupato o vulnerabile quando si utilizza internet;</li> <li>• conoscere e rispettare le norme relative all'uso del cellulare e di altri dispositivi tecnologici portatili all'interno della struttura scolastica.</li> </ul>

<p>GENITORI</p>	<ul style="list-style-type: none"> <li>• Sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle tecnologie dell'Informazione e delle Comunicazioni nella didattica;</li> <li>• seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllare l'utilizzo del pc e di internet;</li> <li>• concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di internet;</li> <li>• fissare delle regole per l'utilizzo del computer e tenere sotto controllo l'uso che i figli fanno di internet e del telefonino in generale.</li> </ul>
-----------------	--

### 1.3 Condivisione e comunicazione della Policy all'intera comunità scolastica

Il documento di E-policy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/le studenti/esse) si faccia a sua volta promotore del documento.

Nella convinzione che un'ampia condivisione su più livelli possa portare ad una maggiore efficacia della E-Safety Policy si possono distinguere tre livelli di comunicazione e diffusione della stessa:

#### 1. *Condividere e comunicare la politica di e-safety agli alunni*

- Tutti gli alunni saranno informati che la rete, l'uso di Internet e di ogni dispositivo digitale saranno controllati dagli insegnanti e utilizzati solo con la loro autorizzazione;
- L'istruzione degli alunni riguardo all'uso responsabile e sicuro di internet precederà l'accesso alla rete;
- L'elenco delle regole per la sicurezza on-line sarà pubblicato in tutte le aule o laboratori con accesso a internet;
- Sarà data particolare attenzione nell'educazione sulla sicurezza agli aspetti per i quali gli alunni risultano più esposti e/o vulnerabili.

#### 2. *Condividere e comunicare la politica di e-safety al personale*

- La linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet sarà discussa negli organi collegiali (consigli di interclasse/intersezione, collegio



dei docenti) e comunicata formalmente a tutto il personale con il presente documento e altro materiale informativo anche sul sito web;

- Il personale docente sarà reso consapevole del fatto che il traffico in internet può essere monitorato e si potrà risalire al singolo utente registrato;
- Un'adeguata informazione/formazione on-line del personale docente nell'uso sicuro e responsabile di internet, sia professionalmente che personalmente, sarà fornita a tutto il personale, anche attraverso il sito web della scuola;
- Il sistema di filtraggio adottato e il monitoraggio sull'utilizzo delle TIC sarà supervisionato dall'Animatore digitale, che segnalerà al DSGA eventuali problemi che dovessero richiedere acquisti o interventi di tecnici;
- Tutto il personale è consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile.

### 3. *Condividere e comunicare la politica di e-safety ai genitori*

- L'attenzione dei genitori sulla sicurezza nell'uso delle tecnologie digitali e di internet sarà sollecitata anche sul sito web della scuola, con la pubblicazione della Policy e link di tutto il materiale informativo inerente l'e-safety messo a disposizione anche dal sito [www.generazioniconnesse.it](http://www.generazioniconnesse.it);
- Accordo di utilizzo accettabile, discusso con gli studenti e i genitori, all'inizio del primo anno, tramite il Patto di Corresponsabilità, che sarà sottoscritto dalle famiglie e rilasciato alle stesse;
- Sarà incoraggiato un approccio di collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di internet in occasione degli incontri scuola-famiglia, assembleari, collegiali e individuali;
- L'animatore digitale, il suo team e i tutti docenti di classe forniranno ai genitori indirizzi sul web relativi a risorse utili per lo studio e a siti idonei ed educativi per gli alunni, sistemi di filtraggio e suggerimenti per un uso sicuro delle tecnologie digitali e di internet anche a casa.

## 1.4 Gestione delle infrazioni alla Policy

La scuola prenderà tutte le precauzioni necessarie per garantire la sicurezza on-line. Tuttavia, a causa della scala internazionale collegata ai contenuti Internet, la disponibilità di tecnologie mobili e velocità di cambiamento, non è possibile garantire che il materiale non idoneo apparirà mai su un computer della scuola o dispositivo mobile. Né la scuola né l'autorità locale possono accettare la responsabilità per il materiale accessibile, o le conseguenze di accesso a Internet. Per il momento la scuola non dispone ancora di una procedura standardizzata e definita per la rilevazione e il monitoraggio degli episodi problematici correlati all'utilizzo di Internet e delle tecnologie digitali.

Il docente responsabile della sicurezza online fungerà da primo punto di contatto per qualsiasi reclamo. Gli episodi rilevati sono segnalati alla Dirigenza Scolastica e vengono gestiti nel rispetto delle prassi interne strutturate. Denunce di cyberbullismo saranno trattate in conformità

con la legge attuale. Reclami relativi alla protezione degli alunni saranno trattati in conformità alle procedure di protezione.

E' stata individuata, sulla base di titoli specifici e formazione adeguata, una figura di docente referente per le attività di prevenzione e contrasto al bullismo e cyberbullismo (Nota MIUR Prot. 964 del 24/02/2017).

In particolare nell'Istituto è attivo uno Sportello d'Ascolto a cui insegnanti e studenti possono rivolgersi per segnalare anche episodi di cyberbullismo o altro e mettere in atto dei percorsi didattico-educativi idonei al superamento delle problematiche emerse. La scuola promuove, non solo la conoscenza, ma anche l'utilizzo di questo servizio, la cui attività è nota alla totalità della comunità scolastica. La figura professionale che opera presso lo sportello di ascolto lavora in stretta collaborazione con gli altri servizi del territorio e di ascolto per bambini e adolescenti.

### *1. Infrazioni e alunni*

Gli interventi correttivi previsti per gli alunni sono rapportati all'età e al livello di sviluppo dell'alunno.

Infatti più gli alunni sono piccoli, più i comportamenti "da correggere" sono dovuti a uno sviluppo cognitivo, affettivo e morale incompleto o a fasi critiche transitorie, che devono essere compresi e orientati proprio dagli educatori, nella prospettiva del raggiungimento di una maggiore consapevolezza e maturità da parte dell'alunno.

Sono previsti pertanto da parte dei docenti provvedimenti disciplinari proporzionati all'età e alla gravità del comportamento, quali:

- il richiamo verbale;
- il richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività gratificante);
- il richiamo scritto con annotazione sul diario;
- la convocazione dei genitori da parte degli insegnanti;
- la convocazione dei genitori da parte del Dirigente scolastico;
- esonero dalla partecipazione ad attività didattico-ricreative (uscite, recite, gite...);
- sospensione temporanea dalle lezioni, per periodi non superiori a quindici giorni, con obbligo di presenza a scuola.

Contestualmente sono previsti interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi dei disagi causati, di ri-definizione 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.

### *2. Infrazioni e docenti*

Il Dirigente scolastico può controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a internet, la posta elettronica inviata/pervenuta a scuola, procedere alla cancellazione di materiali inadeguati o non autorizzati dal sistema informatico della scuola conservandone una copia per eventuali successive investigazioni.

Tutto il personale è tenuto a collaborare con il Dirigente scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio di procedimenti che possono avere carattere organizzativo gestionale, disciplinare, amministrativo, penale, a seconda del tipo o della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

### *3. Infrazioni e genitori*

I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli, se dovessero risultare pericolosi per sé e/o dannosi per gli altri.

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

Il **monitoraggio** dell'implementazione della policy e del suo eventuale aggiornamento sarà svolta ogni anno. Tale monitoraggio sarà curato dal responsabile della Policy di E-Safety con la collaborazione del team dell'Area dell'Innovazione Tecnologica e dei docenti delle classi tramite questionari e conversazioni e infine supervisionato dal Dirigente Scolastico.

Sarà finalizzato a rilevare la situazione iniziale delle classi e gli esiti a fine anno, in relazione all'uso sicuro e responsabile delle tecnologie digitali e di internet. Il monitoraggio sarà rivolto anche agli insegnanti, al fine di valutare l'impatto della policy e la necessità di eventuali miglioramenti.

L'**aggiornamento** della policy sarà curato dal Dirigente e da un docente responsabile della Policy di E-safety che coordini un gruppo di lavoro, il cui compito sia quello di informare e assicurare il coinvolgimento di tutte le parti interessate (studenti, famiglie e personale scolastico) nell'applicazione della Policy e nel monitoraggio della sua implementazione.

## **1.6 Integrazione della Policy con Regolamenti esistenti**

La policy richiede l'integrazione con l'inserimento delle seguenti norme tratte dal Regolamento d'Istituto:

### **ART. 7 – USO DELLE TECNOLOGIE DIGITALI**

1. Riproduzione di immagini. Secondo le norme sulla privacy, è vietata la ripresa di immagini o filmati (con macchina fotografica, videocamera, cellulari...) senza il consenso degli interessati e della presidenza. La mancata ottemperanza alle disposizioni comporterà il temporaneo ritiro dello strumento, eliminazione delle immagini e sanzioni disciplinari;
2. La diffusione esterna (via rete Internet o altro), senza il consenso degli interessati e della scuola, di immagini riprese all'interno della stessa configura grave violazione della legge

sulla privacy con relative sanzioni, anche di carattere penale, previste dalla legge, cui non possono che aggiungersi altrettanto gravi sanzioni disciplinari da parte della scuola;

3. Internet e Social Network. E' rigorosamente vietato l'uso scorretto di Internet e Social Network in merito a tematiche relative all'ambiente scolastico e i suoi componenti: studenti, genitori, insegnanti, personale ausiliario.... Chi dovesse rendersi colpevole di aver postato commenti volgari od offensivi, o immagini non autorizzate, sarà soggetto, oltre alle conseguenze civili ed penali previste dalla legge, a gravi sanzioni disciplinari da parte della scuola. Stessi provvedimenti verranno presi anche nei confronti di chi dovesse inviare sms o mms contenenti volgarità o ingiurie.

## **ART. 8 – USO DEL CELLULARE**

1. Si ribadisce la puntuale applicazione della normativa vigente (DPR 249/1998, DPR 235/2007, Direttiva Ministeriale 15.03.2007), pertanto l'uso del cellulare in quanto tale non è consentito per ricevere/effettuare chiamate, SMS o altro tipo di messaggistica. Il divieto non si applica soltanto all'orario delle lezioni ma è vigente anche negli intervalli e nelle altre pause dell'attività didattica.
2. La comunicazione con le famiglie, per qualsiasi urgenza, è sempre garantita attraverso il telefono della scuola. I docenti possono derogare a tale disposizioni, consentendo l'uso del cellulare, in caso di particolari situazioni non risolvibili in altro modo;
3. Le famiglie sono invitate a collaborare strettamente con l'Istituto, nello spirito della corresponsabilità educativa, evitando, ad esempio, di inviare messaggi o effettuare chiamate ai telefoni dei propri figli, durante l'orario scolastico;
4. Gli alunni sono tenuti a mantenere i loro telefoni spenti durante l'intera permanenza a scuola;
5. Eventuali fotografie o riprese fatte con i videotelefonini all'interno della scuola e nelle sue pertinenze, senza il consenso scritto della/e persona/e, si configurano come violazione della privacy e quindi perseguibili per legge.
6. I genitori rispondono direttamente dell'operato dei propri figli nel caso in cui gli stessi arrechino danno a se stessi o agli altri con obbligo di risarcimento.

## **2. Formazione e Curricolo**

### **2.1 Curricolo sulle competenze digitali per gli studenti**

Il Curricolo della scuola del primo ciclo di istruzione sulle competenze digitali per gli alunni è trasversale alle discipline previste dalle Indicazioni Nazionali: la competenza digitale è ritenuta dall'Unione Europea competenza chiave (Raccomandazione 2006/962/CE), per la sua importanza e pervasività nel mondo d'oggi necessaria per il *lifelong learning*, ovvero il complesso delle competenze necessarie per esercitare pienamente il diritto di cittadinanza nella società.

L'approccio per discipline scelto dalle Indicazioni non consente di declinarla con le stesse modalità con cui si possono declinare le competenze chiave nelle quali trovano riferimento le

discipline formalizzate. Si ritrovano abilità e conoscenze che fanno capo alla competenza digitale in **tutte** le discipline e **tutte** concorrono a costruirla. Competenza digitale significa padroneggiare certamente 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. Esse trovano, tuttavia, una declinazione più specifica all’interno del curriculum d’Istituto.

## **2.2 Formazione dei docenti sull’utilizzo e l’integrazione delle TIC nella didattica**

Il corpo docente ha partecipato a corsi di formazione anche nell’ambito di piani nazionali, oltre che ad iniziative organizzate dall’istituzione o dalle scuole associate in rete e possiede generalmente una buona base di competenze e nel caso delle figure di sistema, anche di carattere specialistico.

E’ inoltre disponibile ad aggiornarsi per mantenere al passo la propria formazione, in rapporto al rinnovo della dotazione multimediale.

Il percorso complesso della formazione specifica dei docenti sull’utilizzo delle TIC nella didattica, non esauribile nell’arco di un anno scolastico, può pertanto prevedere momenti di autoaggiornamento, momenti di formazione personale o collettiva anche all’interno dell’istituto, con la condivisione delle conoscenze dei singoli e la fruizione dei materiali messi a disposizione dall’Animatore Digitale e il suo team sulle bacheche virtuali appositamente create sul sito della scuola.

## **2.3 Formazione dei docenti sull’utilizzo consapevole e sicuro di Internet e delle tecnologie digitali**

Anche il percorso della formazione specifica dei docenti sull’utilizzo consapevole e sicuro di Internet, può prevedere momenti di autoaggiornamento, momenti di formazione personale o collettiva di carattere permanente, legata all’evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono sempre di più ed autonomamente anche i ragazzi.

Sarà predisposta una bacheca online collegata alla homepage del sito della scuola ([www.iismargheritahack.edu.it](http://www.iismargheritahack.edu.it)) per la messa a disposizione e la condivisione di materiali per l’aggiornamento sull’utilizzo consapevole e sicuro di internet. Qui sarà possibile trovare materiali informativi sulla sicurezza in internet per l’approfondimento personale, per le attività con gli studenti e gli incontri con i genitori, costituiti da guide in pdf, video, manuali a fumetti, link a siti specializzati e contributi della Polizia di Stato, dell’Arma dei Carabinieri, di Telefono Azzurro, dal sito “Generazioni connesse”, ecc.

## **2.4 Sensibilizzazione delle famiglie**

La scuola si impegna alla diffusione delle informazioni e delle procedure contenute nel documento E-Safety Policy per portare a conoscenza delle famiglie il regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e prevenire i rischi legati a un utilizzo non corretto di internet.

L'Istituto attiverà iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC e della rete, promuovendo la conoscenza delle numerose situazioni di rischio online. A tal fine sono previsti incontri fra docenti e genitori per la diffusione del materiale informativo sulle tematiche trattate, messo a disposizione dai siti specializzati e dalle forze dell'ordine.

Saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso di cellulari e smartphone o delle chat line o social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo. Sul sito scolastico e sulla relativa bacheca virtuale relativa a "Generazioni connesse" saranno messi in condivisione materiali dedicati ad alunni e alle famiglie come guide in formato .pdf e video che possono fornire spunti di approfondimento e confronto.

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

### **3.1 Accesso ad internet: filtri, antivirus e sulla navigazione**

L'accesso a internet è garantito sia nella sede centrale sia nella sede associata del comune di Rignano Flaminio.

L'utilizzo di internet da parte dei docenti è consentito in tutta la struttura. Nel laboratorio multimediale le postazioni degli studenti (client) sono dotate di due account con i quali effettuare l'accesso: "docente" e "alunno". L'account "docente" è dotato di una password fornita dall'Animatore digitale ai soli utenti adulti (personale scolastico); l'account "alunno" è impostato con restrizioni di navigazione attraverso filtri specifici. Le postazioni degli alunni (client) sono, infatti, occasionalmente utilizzate anche dai docenti, o da utenti esterni in occasione di corsi di aggiornamento, a cui accede personale scolastico da altre scuole o in occasione di concorsi pubblici. I docenti hanno piena autonomia nel collegamento ai siti web.

Le postazioni non sono dotate di webcam.

L'Animatore digitale periodicamente provvede alla manutenzione e all'aggiornamento del sistema informatico del laboratorio, ove necessario richiedendo l'intervento di tecnici esterni.

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

L'accesso al sistema informatico per la didattica e per la compilazione del registro elettronico è consentito al personale docente attraverso l'assegnazione di una password comune a tutti i docenti da parte dell'Animatore digitale. A breve sarà disponibile un registro nel laboratorio multimediale dove i docenti potranno registrare il proprio accesso, scrivendo la data e l'orario di utilizzo

Non vi è un backup dei file elaborati, se non quello operato dai docenti interessati sui supporti rimovibili personali. Le postazioni del laboratorio funzionano come stazioni di lavoro e non come archivi.

### **3.3 E-mail**

L'account di posta elettronica è solo quello istituzionale utilizzato ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita. L'eventuale invio o ricevimento di posta a scopi didattici avverrebbe solo su autorizzazione del Dirigente scolastico e operativamente sarebbe svolto dall'assistente amministrativo addetto. La posta elettronica è protetta da antivirus, e quella certificata anche dall'antispam.

### **3.4 Blog e sito web della scuola**

La scuola attualmente ha un sito web. Tutti i contenuti del settore didattico sono pubblicati direttamente e sotto supervisione di un docente membro dell'Area dell'Innovazione Tecnologica, che ne valuta con il Dirigente scolastico la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy, ecc.

Tra i progetti futuri è contemplata anche la possibilità di aprire un Blog a scopo didattico-laboratoriale con la partecipazione attiva degli studenti.

### **3.5 Social network**

Attualmente nella didattica non si utilizzano social network.

### **3.6 Protezione dei dati personali**

Il personale scolastico è "incaricato del trattamento" dei dati personali (degli alunni, dei genitori, ecc.), nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione). Tutto il personale incaricato riceve poi istruzioni particolareggiate applicabili al trattamento di dati personali su supporto cartaceo e su supporto informatico, ai fini della protezione e sicurezza degli stessi.

Viene inoltre fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori.

## **4. Strumentazione personale**

### **4.1 Per gli studenti: gestione degli strumenti personali - cellulari, tablet ecc..**

Non è consentito l'uso di cellulari e smartphone personali.

È consentito l'uso di tablet all'interno di progetti d'Istituto autorizzati dal Collegio Docenti.

#### **4.2 Per i docenti: gestione degli strumenti personali - cellulari, tablet ecc..**

Durante l'orario di servizio è vietato l'uso del cellulare tranne per comunicazioni personali di carattere urgente, mentre è permesso l'uso di altri dispositivi elettronici personali (come computer e tablet) per attività funzionali all'insegnamento, ad integrazione di quelli scolastici disponibili.

#### **4.3 Per il personale della scuola: gestione degli strumenti personali - cellulari, tablet ecc.**

È vietato l'uso del cellulare per il restante personale scolastico durante l'orario di servizio, tranne per comunicazioni personali di carattere urgente.

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

#### **5.1 *Prevenzione***

##### **5.1.1 Rischi**

I rischi effettivi che si possono correre a scuola nell'utilizzo delle TIC da parte degli studenti derivano da un uso non corretto dei pc della scuola collegati alla rete oppure dall'uso non responsabile dello smartphone anche a scuola, dove esso è severamente vietato.

Il rapporto tra giovani e nuove tecnologie va concettualizzato in ottica di rischi e opportunità come facce di una stessa medaglia. Recenti ricerche (EU kids online) hanno infatti mostrato che all'aumentare delle opportunità aumentano anche i rischi, suggerendo quindi di lavorare a strategie di mediazione e prevenzione per un uso consapevole e creativo. Per "uso responsabile" si intende utilizzare uno strumento in modo sicuro e consapevole: significa in primo luogo conoscerlo tecnicamente, cioè avere dimestichezza con tutte le sue potenzialità e "implicazioni". Ma questo elemento da solo non basta: se Internet e cellulari possono essere considerati qualcosa di più che semplici strumenti, in quanto sono in grado di collocarci all'interno di un sistema di relazioni, di una "piazza", il loro utilizzo responsabile implica la capacità di gestire con un certo grado di lucidità i rapporti che si sviluppano in tale ambiente. Essere consapevoli, ad esempio, di subire il fascino di un incontro in rete, o di sentirsi offesi per il comportamento online di qualche amico, o del turbamento prodotto dalla visione di certe immagini, o del tipo di influenza che possono produrre determinate informazioni.

Tra le tipologie più ricorrenti di rischi legati alle attività online, si possono individuare:



- **il Cyberbullismo**

È una forma di prepotenza virtuale attuata attraverso l'uso di Internet e delle tecnologie digitali. Come il bullismo tradizionale è una forma di prevaricazione e di oppressione reiterata nel tempo, perpetrata da una persona o da un gruppo di persone più arroganti nei confronti di un'altra percepita come più debole;

- **l'Adescamento online**

Gli adulti interessati sessualmente a bambini/e e adolescenti possono utilizzare la Rete per entrare in contatto con loro e instaurare gradualmente una relazione intima e/o sessualizzata attraverso il grooming (dall'inglese "groom" - curare, prendersi cura), una tecnica di manipolazione psicologica, che gli adulti potenziali abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive;

- **il Sexting**

Rappresenta la 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;

- **la Pornografia**

Recenti ricerche hanno sottolineato come la maggior parte degli adolescenti reperisca in Rete informazioni inerenti la sessualità, col rischio, spesso effettivo, del diffondersi di informazioni scorrette e/o l'avvalorarsi di falsi miti;

- **Pedopornografia**

Con questo termine si intende qualsiasi foto o video di natura sessuale che ritrae persone minorenni;

- **il Gioco d'azzardo o Gambling**

È il puntare o lo scommettere una data somma di denaro, o oggetto di valore, sull'esito di un gioco che può implicare la dimostrazione di determinate abilità o basarsi sul caso;

- **la Dipendenza da Internet (Internet Addiction)**

I/le ragazzi/e che ne soffrono sono spesso inconsapevoli ma, lontani dalla Rete, manifestano presto insofferenza, irascibilità e altri sintomi di disagio;

- **l'Esposizione a contenuti dannosi o inadeguati** (es. contenuti razzisti, commenti che mitizzano atti d'animo depressivi o che promuovono comportamenti alimentari scorretti, ecc.).

### 5.1.2 Azioni

Le azioni previste di **prevenzione** in merito ai rischi che si possono incorrere per un uso non responsabile e corretto delle TIC sono:

- Informare e formare i docenti, i genitori, il personale ATA e gli studenti sui rischi che un uso non sicuro delle nuove tecnologie può favorire;
- Attivazione di progetti che sviluppino una convivenza efficace attraverso la gestione delle emozioni (proprie e altrui) e l'accettazione della diversità;
- Promuovere la diffusione della conoscenza delle Linee di orientamento per azioni di prevenzione e di contrasto al bullismo e al cyberbullismo del MIUR;
- Non consentire l'utilizzo del cellulare personale degli alunni a scuola, in quanto per assolvere a ogni comunicazione urgente con i genitori o con chi ne fa le veci è sempre disponibile il telefono della scuola supervisionato dal collaboratore scolastico o dal personale di segreteria, che prima di passare la telefonata si accerta dell'identità dell'interlocutore;
- Utilizzare filtri, software che impediscono il collegamento ai siti web per adulti (black list);

Le azioni di contenimento degli incidenti previste sono le seguenti:

- Se la condotta incauta dell'alunno consiste nel fare circolare immagini imbarazzanti, di natura sessuale su internet (Sexting), è necessario rimuoverle: contattare il service provider e se il materiale postato viola i termini e le condizioni d'uso del sito chiedere di rimuoverle.
- Se l'alunno viene infastidito od offeso (Cyberbullismo), suggerirgli di modificare i dettagli del proprio profilo sistemandolo su "privato", in modo tale che solo gli utenti autorizzati siano in grado di vederlo (MSN messengers, siti social network, Skype etc.), o suggerirgli di bloccare o ignorare particolari mittenti, di cancellare il loro nominativo dalla lista degli amici con i quali regolarmente chatta, di inserire il compagno o la persona che offende, per quanto riguarda l'e-mail, tra gli indesiderati;
- Consigliare di cambiare il proprio indirizzo e-mail, contattando l'e-mail provider, di scaricare un'applicazione che blocchi chiamate e messaggi da numeri indesiderati o, se necessario, cambiare il numero di cellulare;
- Fare cancellare il materiale offensivo dal telefonino, facendo intervenire i genitori, e chiedere agli studenti di indicare a chi e dove lo hanno spedito per farlo fare anche gli altri, e conservare una copia di detto materiale se necessario per ulteriori indagini;
- Contattare la polizia postale e/o giudiziaria se si ritiene che il materiale offensivo sia illegale. In caso di foto e video pedopornografici, confiscare il telefonino o altri dispositivi ed **evitare di eseguire download, perché reato.**

## 5.2 Rilevazione

### 5.2.1 Che cosa segnalare

Confrontandosi periodicamente con gli alunni sui rischi delle comunicazioni on-line, i minori possono riferire di fatti o eventi personali o altrui che "allertano" l'insegnante.

I contenuti "pericolosi" comunicati/ricevuti a/da altri, messi/scaricati in rete, sono tracce che possono comprovare l'utilizzo incauto, scorretto o criminoso degli strumenti digitali e sono una

“prova” di quanto riferito presente nella memoria degli strumenti tecnologici utilizzati che può essere mostrata spontaneamente dall’alunno o presentata da un reclamo dei genitori o anche notata dall’insegnante che si accorge dell’infrazione in corso.

Essi possono classificarsi in tre tipologie:

- Contenuti afferenti alla **privacy**: foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, ecc.;
- Contenuti afferenti all’**aggressività** o alla **violenza**: messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.;
- Contenuti afferenti alla **sessualità**: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), ecc.

### 5.2.2 Come segnalare: quali strumenti e a chi

**I contenuti “prova”** di un utilizzo incauto, scorretto o criminoso degli strumenti digitali devono essere conservati dal personale scolastico per far conoscere l’accaduto, in base alla gravità, in primis al Dirigente Scolastico che coinvolgerà i genitori degli alunni protagonisti di una condotta pericolosa, mentre per le condotte criminose sarà debitamente informata la polizia giudiziaria.

**In mancanza di prove**, ma solo delle testimonianze dell’alunno, riferite a fatti accaduti anche al di fuori del contesto scolastico, le notizie raccolte sono comunicate ai genitori e per fatti rilevanti al Dirigente Scolastico, per quelle criminose, anche alla polizia giudiziaria. In particolare la segnalazione viene fatta ad entrambe le famiglie, se oltre la vittima anche l’autore della condotta negativa è un altro alunno.

Per le segnalazioni di fatti rilevati sono previsti i seguenti **strumenti** che i docenti possono utilizzare sulla base della gravità dell’accaduto:

- Annotazione del comportamento sul registro e comunicazione scritta ai genitori, che la devono restituire vistata;
- Convocazione scritta e colloquio con i genitori degli alunni, da parte dei docenti;
- Relazione scritta al Dirigente Scolastico.

In base all’urgenza le comunicazioni formali possono essere precedute da quelle informali, effettuate per le vie brevi.

Per i reati **meno gravi** la legge rimette ai genitori degli alunni la scelta di richiedere la punizione del colpevole, attraverso la querela.

Mentre per i reati **più gravi** (es. pedopornografia) gli operatori scolastici hanno **l'obbligo** di effettuare la denuncia all'autorità giudiziaria.

In particolare per i **fatti criminosi**, ai fini della denuncia, la relazione deve essere redatta nel modo più accurato possibile, indicando i seguenti elementi: il fatto, il giorno dell'acquisizione del fatto nonché le fonti di prova già note e per quanto possibile, le generalità, il domicilio e quant'altro di utile a identificare la persona alla quale il reato è attribuito, la persona offesa, e tutti coloro che sono in grado di riferire circostanze rilevanti per la ricostruzione del fatto.

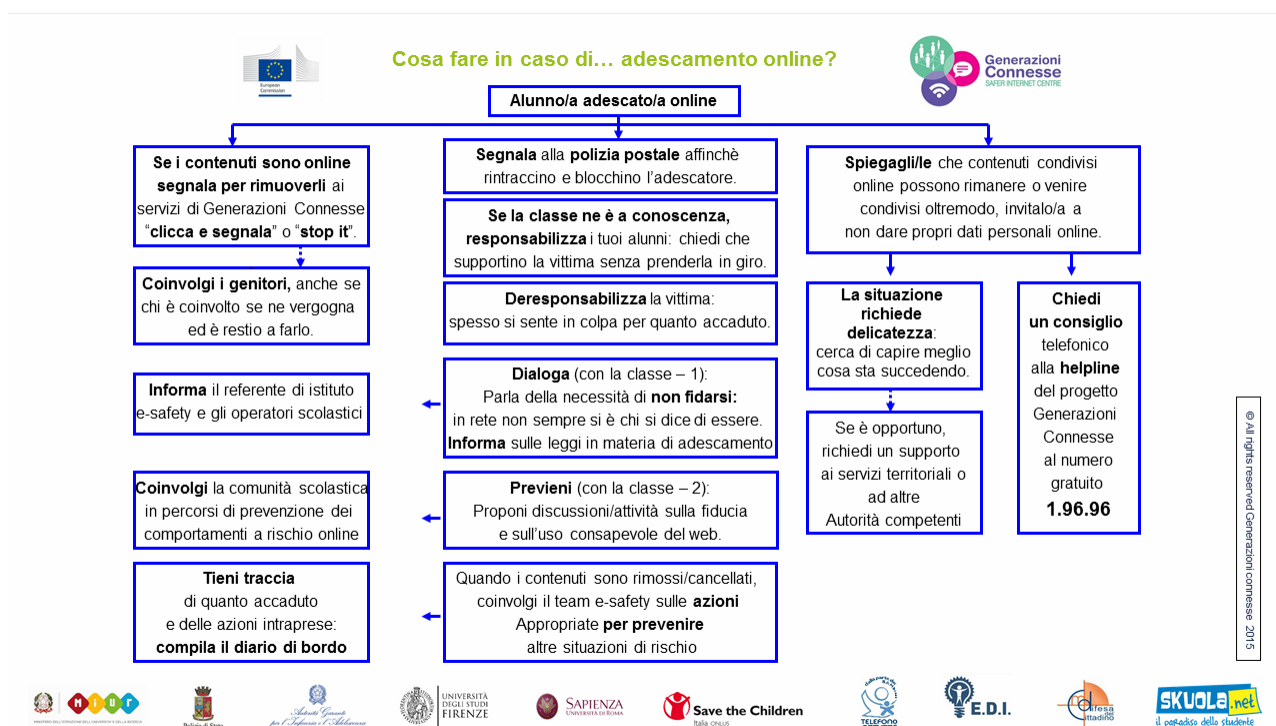
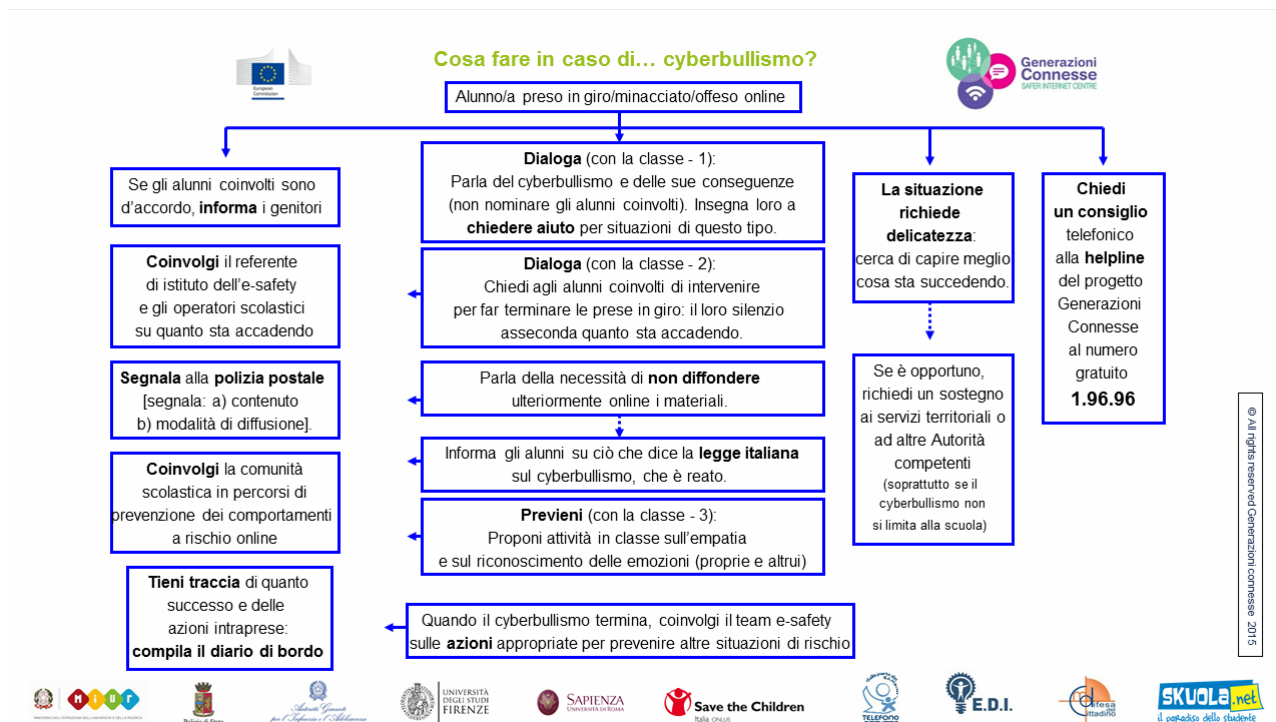
Inoltre per episodi di **bullismo e cyberbullismo** i docenti di classe raccoglieranno le segnalazioni e le comunicheranno alla docente referente che definirà un piano d'azione specifico in base alla problematica emersa.

### 5.2.3 Come gestire le segnalazioni

Il docente responsabile della sicurezza online fungerà da primo punto di contatto per qualsiasi reclamo. Gli episodi rilevati sono segnalati alla Dirigenza Scolastica e vengono gestiti nel rispetto delle prassi interne strutturate. Denunce di cyberbullismo saranno trattate in conformità con la legge attuale. Reclami relativi alla protezione dei bambini saranno trattati in conformità alle procedure di protezione dell'infanzia.

## 5.3 Gestione dei casi

### 5.3.1 Definizione delle azioni da intraprendere a seconda della specifica del caso



## **6. Procedure operative per la gestione delle infrazioni alla Policy**

Non sono state ancora prodotte e si provvederà ad inserirli al primo aggiornamento della Policy.

## **7. Procedure operative per la protezione dei dati personali**

Per il trattamento dei dati personali la scuola fa riferimento alla seguente informativa, qualora i genitori non fossero d'accordo devono segnalare il loro dissenso, previa comunicazione scritta.

### **INFORMATIVA EX. ART. 13 D.LGS. N.196/2003 PER IL TRATTAMENTO DEI DATI PERSONALI DEGLI ALUNNI E DELLE FAMIGLIE**

Gentile signore/a,

secondo le disposizioni del decreto Legislativo 30 giugno 2003, n. 196 ( Codice in materia di protezione dei dati personali) nel seguito indicato sinteticamente come Codice il trattamento dei dati personali che riguardano i componenti della sua famiglia sarà improntato ai principi di liceità e trasparenza, a tutela della vostra riservatezza e dei vostri diritti.

Ai sensi dell'articolo 13 del Codice, le forniamo, quindi, le seguenti informazioni sul trattamento dei dati più sopra menzionati:

1. nel corso del rapporto con la presente Istituzione scolastica, i dati personali verranno trattati dal personale della scuola nell'ambito delle finalità istituzionali, che sono quelle relative all'istruzione ed alla formazione degli alunni e quelle amministrative ad esse strumentali, così come definite dalla normativa vigente (R.D. n. 653/1925, D.Lgs. n. 297/1994, D.P.R. n. 275/1999; Decreto Interministeriale 1 febbraio 2001, n. 44 e le norme in materia di contabilità generale dello Stato; Legge n. 104/1992, Legge n. 53/2003, D.Lgs. n. 165/2001, Dlgs 196/2003, D.M 305/2006; Dlgs 76/05; Dlgs 77/05; Dlgs 226/05; D.Lgs. n. 151/2001, i Contratti Collettivi di Lavoro Nazionali ed Integrativi stipulati ai sensi delle norme vigenti; D.P.C.M. 23 febbraio 2006, n. 185; D.P.R. 20 marzo 2009,n.89; Legge 170 dell'8.10.2010; D.M. n. 5669 12 luglio 2011; tutta la normativa collegata alle citate disposizioni);
2. i dati personali definiti come "dati sensibili" o come "dati giudiziari" dal Codice saranno trattati esclusivamente dal personale della scuola, appositamente incaricato, secondo quanto previsto dalle disposizioni di legge e di regolamento citate al precedente punto 1 e nel rispetto del principio di stretta indispensabilità dei trattamenti. Le ricordiamo che i dati sensibili sono quei dati personali "idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale". I dati giudiziari sono quei dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o

la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

3. i dati personali potranno essere soggetti pubblici (quali, ad esempio, ASL, Comune, Provincia, Ufficio scolastico regionale, Ambiti Territoriali, organi di polizia giudiziaria, organi di polizia tributaria, guardia di finanza, magistratura) nei limiti di quanto previsto dalle vigenti disposizioni di legge e di regolamento e degli obblighi conseguenti per codesta istituzione scolastica; i dati relativi agli esiti scolastici degli alunni potranno essere pubblicati mediante affissione all'albo della scuola secondo le vigenti disposizioni in materia;
4. i dati da Lei forniti potranno essere comunicati a terzi soggetti che forniscono servizi a codesta Istituzione scolastica quali agenzie di viaggio e strutture ricettive (esclusivamente in relazione a gite scolastiche, viaggi d'istruzione e campi scuola), imprese di assicurazione (in relazione a polizze in materia infortunistica), eventuali ditte fornitrici di altri servizi (quali ad esempio servizi di mensa). La realizzazione di questi trattamenti costituisce una condizione necessaria affinché l'interessato possa usufruire dei relativi servizi;
5. si fa inoltre presente che è possibile che:
  - ✓ foto di lavori e di attività didattiche afferenti ad attività istituzionali della scuola inserite nel Piano Triennale dell'Offerta Formativa (quali ad esempio foto relative ad attività di laboratorio, visite guidate, premiazioni, partecipazioni a gare sportive, ecc.) vengano pubblicate sul sito istituzionale e/o sul giornalino della scuola;
  - ✓ vengano effettuate durante l'anno foto di classe;
  - ✓ vengano effettuate riprese, da parte della scuola, di alcune attività didattiche. In questo ultimo caso le immagini saranno adeguatamente conservate presso i locali della scuola, non saranno diffuse e ad esse avrà accesso solo il personale della scuola appositamente incaricato.

In caso di pubblicazione di immagini e/o video sul sito istituzionale il trattamento avrà natura temporanea dal momento che le suddette immagini e video resteranno sul sito solo per il tempo necessario per la finalità cui sono destinati. Nei video e nelle immagini di cui sopra i minori saranno ritratti solo nei momenti "positivi" (secondo la terminologia utilizzata dal Garante per la protezione dei dati personali e dalla Carta di Treviso del 5 ottobre 1990 e successive integrazioni) legati alla vita della scuola: apprendimento, recite scolastiche, competizioni sportive, ecc.

Si fa presente che per ulteriori informazioni e delucidazioni, o per segnalare la volontà di non aderire a determinate iniziative o servizi tra quelli indicati ai punti 4 e 5 del presente documento, è possibile rivolgersi al responsabile del trattamento dei dati personali della scuola, indicato al punto 13 del presente atto.

6. Ad eccezione di quanto previsto ai punti 4 e 5 del presente documento, il conferimento dei dati richiesti e il conseguente trattamento sono obbligatori, in quanto previsti dalla normativa citata al precedente punto 1; l'eventuale rifiuto a fornire tali dati potrebbe comportare il mancato perfezionamento dell'iscrizione e l'impossibilità di fornire all'alunno tutti i servizi necessari per garantire il suo diritto all'istruzione ed alla formazione;
7. il trattamento sarà effettuato sia con strumenti cartacei che elettronici, nel rispetto delle misure di sicurezza indicate dal Codice;
8. i dati sensibili e giudiziari non saranno oggetto di diffusione; tuttavia, alcuni di essi potranno essere comunicati ad altri soggetti pubblici nella misura strettamente

indispensabile per svolgere attività istituzionali previste dalle vigenti disposizioni in materia sanitaria, previdenziale, tributaria, giudiziaria e di istruzione, nei limiti previsti dal D.M 305/2006, pubblicato sulla G.U. n° 1 del 15-01-07;

9. l'istituzione scolastica può comunicare o diffondere, anche a privati e per via telematica, dati relativi agli esiti scolastici degli alunni per finalità di orientamento, formazione e inserimento professionale, solo su richiesta degli interessati, secondo quanto disposto dall'articolo 96 comma 1 del Codice;
10. per consentire ai genitori l'assolvimento dell'obbligo di garantire l'istruzione dei figli maggiorenni, che siano ancora non autosufficienti e conviventi, così come indicato dalle norme vigenti (cfr cod. civ. articoli 148 cc e 155-quinquies) e dai pronunciamenti giurisprudenziali (cfr, ad esempio, Corte Cassazione n. 04765 del 3 aprile 2002), è permesso ai genitori medesimi l'accesso alle informazioni riguardanti il rendimento scolastico e la frequenza dei figli maggiorenni rientranti nelle categorie più sopra indicate (non autosufficienti e ancora conviventi).

Il Titolare del trattamento è: l'Istituto d'Istruzione Superiore "Margherita Hack" di Morlupo, rappresentato dal Dirigente Scolastico Prof.re Gianfranco Cherubini. Al Titolare del trattamento o al Responsabile Lei potrà rivolgersi senza particolari formalità, per far valere i suoi diritti, così come previsto dall'articolo 7 del Codice (e dagli articoli collegati), che per sua comodità riproduciamo integralmente:

Art. 7 (Diritto di accesso ai dati personali ed altri diritti)

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. L'interessato ha diritto di ottenere l'indicazione:
  - a. dell'origine dei dati personali;
  - b. delle finalità e modalità del trattamento;
  - c. della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
  - d. degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
  - e. dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.
3. L'interessato ha diritto di ottenere:
  - a. l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
  - b. la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
  - c. l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.



4. L'interessato ha diritto di opporsi, in tutto o in parte:
- a. per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
  - b. al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Inoltre si fa presente che in occasione di attività particolari l'Istituto provvede a realizzare un'autorizzazione specifica, come la seguente:

I genitori dell'alunno/a,.....

della classe....., sezione..... dell'Istituto d'Istruzione Superiore "Margherita Hack" di Morlupo(Roma)

padre:.....

madre:.....

autorizzano gli insegnanti ad effettuare foto e riprese video del proprio figlio, in orario scolastico, finalizzate alla promozione del crowdfunding dell'Istituto per realizzare un laboratorio didattico. Tali riprese verranno utilizzate sui social media a scopo di diffusione del progetto.

In fede

Firma padre.....

Firma madre.....

Morlupo,

---

## **8. Procedure operative per la rilevazione, il monitoraggio e la gestione delle segnalazioni**

Non sono state ancora prodotte e si provvederà ad inserirli al primo aggiornamento della Policy.

## **9. Procedure operative per la gestione dei casi**

Non sono state ancora prodotte e si provvederà ad inserirli al primo aggiornamento della Policy.

## **10. Protocolli siglati con le forze dell'ordine e i servizi del territorio per la gestione condivisa dei casi**

Non vi sono protocolli siglati ma ricorrenti forme di collaborazione nella prevenzione e contrasto del bullismo e del cyberbullismo da parte dell'Ente Locale e del Comando dei Carabinieri.

Il Dirigente Scolastico  
Prof.re Gianfranco Cherubini  
*Firma autografa sostituita a mezzo stampa ai sensi e per  
gli effetti dell'art. 3, co. 2, D.Lgs. 39/93*