

## POLICY DI E-SAFETY

A.S. 2017-2018

### INDICE

#### 1. Introduzione

- 1.1.Scopo della 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 Sito web della scuola
- 3.5 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
- 5.2 Azioni
- 5.3 Rilevazione e gestione dei casi

#### 6. Annessi

1. Procedure operative per la gestione dei casi.
2. Diario di bordo per la registrazione di casi
3. Modulo di segnalazione dei casi

# 1. Introduzione

## 1.1.Scopo della policy

La presenza sempre più diffusa delle tecnologie digitali nella vita quotidiana dei più giovani, compresi gli ambienti scolastici, apre nuove opportunità, ma pone nuove attenzioni dal punto di vista del loro uso sicuro, consapevole e positivo. Inoltre, lo sviluppo e l'integrazione dell'uso delle TIC, ed in particolare di Internet, nella didattica, offrono le condizioni e l'occasione per una trasformazione dell'insegnamento e dell'apprendimento nelle scuole. Allo stesso tempo, l'uso sempre più pervasivo di piattaforme in rete e dispositivi portatili ha esposto gli utenti e in particolare i minori, i soggetti con divario digitale o con limitate competenze informatiche, a nuovi rischi, tanto più rilevanti quanto meno è diffusa una cultura relativa ai modi legittimi di usare la rete e alla consapevolezza delle funzioni rese possibili.

Sono questi i motivi che hanno indotto la nostra scuola ad aderire, nell'ambito del PNSD, al progetto "Generazioni Connesse" e ad elaborare una Policy di E-Safety, un documento che stabilisca i principi fondamentali di tutti i membri della comunità scolastica per quanto concerne l'utilizzo di tecnologie; per salvaguardare e proteggere i bambini, i ragazzi e lo staff dell'Istituto; assistere il personale della scuola a lavorare in modo sicuro e responsabile, monitorare i propri standard e le prassi; impostare chiare aspettative di comportamento e/o codici di condotta rilevanti per un uso responsabile di Internet a scopo didattico, personale o ricreativo; affrontare gli abusi online come il cyberbullismo, che sono riferimenti incrociati con le altre politiche della scuola; garantire che tutti i membri della comunità scolastica siano consapevoli del fatto che il comportamento illecito o pericoloso è inaccettabile e che saranno intraprese le opportune azioni disciplinari e giudiziarie.

L'eSafety Policy nel nostro Istituto intende dare un impulso allo sviluppo di una cultura d'uso corretto e consapevole di Internet, sia tramite il richiamo a norme vigenti, sia con l'indicazione di prassi opportune per un uso sempre più professionale da parte di tutto il personale e per la prevenzione dei rischi e la gestione delle emergenze.

## 1.2 Ruoli e responsabilità

Gli adulti hanno un ruolo fondamentale nel garantire che bambini e adolescenti siano in grado di utilizzare le tecnologie digitali e che lo facciano in modo appropriato e sicuro, ruolo che vede coinvolta a pieno titolo la comunità scolastica nel suo complesso, genitori inclusi.

La scuola pertanto si impegna a:

- fornire agli alunni gli strumenti per conoscere e utilizzare tutte le potenzialità formative delle tecnologie digitali;
- renderli consapevoli anche dei rischi a cui sono esposti con un uso non corretto;
- intervenire e gestire tutti quei casi che minacciano la sicurezza dei ragazzi in rete;
- garantire che la scuola utilizzi un Internet Service filtrato approvato, conforme ai requisiti di legge vigenti;
- assicurare che il personale riceva una formazione adeguata per svolgere i ruoli di sicurezza on-line e per la formazione di altri colleghi;
- riconoscere come responsabili della sicurezza online il Dirigente Scolastico, il DSGA e il DOP (Data Protection Officer - Responsabile della protezione dei dati personali), per la nomina del quale è stato emanato con circolare del 26/04/2018 avviso interno;
- attivare procedure da seguire in caso di infrazione della E-Safety Policy;

- monitorare la sicurezza online;
- assicurare che l'educazione alla sicurezza online sia incorporata in tutti i programmi di studi;
- supervisionare e guidare gli alunni con cura quando sono impegnati in attività di apprendimento che coinvolgono la tecnologia on-line, come l'uso di telefoni cellulari, fotocamere e dispositivi portatili;
- garantire che tutto il personale sia a conoscenza delle procedure che devono essere seguite in caso di incidente per la sicurezza online;
- controllare probabili azioni di cyberbullismo e segnalare qualsiasi abuso sospetto o problema;
- pubblicare la E-Safety Policy sul sito della scuola e favorire la sua diffusione;
- garantire che tutti i dati relativi agli alunni pubblicati sul sito siano tutelati;
- garantire che gli alunni siano pienamente consapevoli delle capacità di ricerca e siano pienamente consapevoli dei problemi legali relativi ai contenuti elettronici come ad esempio le leggi sul copyright;
- garantire che le comunicazioni digitali con gli studenti siano a livello professionale e solo attraverso i sistemi scolastici, non attraverso meccanismi personali, per esempio e-mail, telefoni cellulari, ecc.

Gli alunni si impegnano a:

- leggere, comprendere ed accettare la E-Safety Policy;
- partecipare con interesse a tutte le iniziative a essi rivolte;
- capire l'importanza di segnalare abusi, o l'uso improprio o l'accesso a materiali inappropriati;
- sapere quali azioni intraprendere se loro o qualcuno che conoscono si sente preoccupato o vulnerabile quando si utilizza la tecnologia on-line;
- capire l'importanza di adottare buone pratiche di sicurezza on-line quando si usano le tecnologie digitali nell'ambito scolastico e fuori dalla scuola;
- assumersi la responsabilità di conoscere i benefici e i rischi di utilizzo di Internet e di altre tecnologie in modo sicuro, sia a scuola che a casa.

Le famiglie si impegnano a:

- collaborare con la scuola per sensibilizzare i propri figli di fronte a queste tematiche;
- partecipare a tutte le iniziative che li vedano direttamente coinvolti;
- sostenere la scuola nel promuovere la sicurezza online e approvare l'accordo di E-Safety Policy con la scuola;
- accedere al sito web della scuola in conformità con quanto stabilito dalla stessa;
- assicurarsi che la scuola abbia preso tutte le precauzioni necessarie circa un uso corretto della tecnologia da parte degli alunni.

### **1.3 Condivisione e comunicazione della policy all'intera comunità scolastica**

La E-Safety Policy d'Istituto si applica a tutti i membri della scuola, compreso il personale, gli studenti, i genitori, gli utenti della comunità, che ne hanno accesso.

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

- pubblicazione della E-Safety Policy sul sito della scuola;
- accordo di utilizzo accettabile, discusso con gli studenti e i genitori, all'inizio del primo anno, tramite il Patto di Corresponsabilità, che sarà sottoscritto dalle famiglie e rilasciato alle stesse; accordo di utilizzo accettabile rilasciato al personale scolastico;
- informative ai genitori sulla tutela della privacy e sugli strumenti di prevenzione, segnalazione e gestione di situazioni problematiche relative all'uso delle tecnologie digitali;
- incontri formative rivolti a docenti, genitori e alunni

## **1.4 Gestione delle infrazioni alla policy**

Nella scuola si istituirà un apposito organo di garanzia costituito da un gruppo di docenti che, tenuto conto delle procedure operative individuate per la gestione delle infrazioni alla Policy, valuterà le infrazioni e deciderà le modalità di azione più opportune per intervenire.

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.

Al personale e agli alunni saranno date informazioni sulle infrazioni in uso e le eventuali sanzioni. Le suddette sanzioni includono:

- informare il docente della classe, il docente responsabile della sicurezza on line (o il DSGA), il Dirigente Scolastico;
- informare i genitori o i tutori;
- il ritiro del cellulare fino a fine giornata;
- la rimozione di Internet o del computer di accesso per un periodo;
- la comunicazioni alle autorità competenti.

Il docente responsabile della sicurezza on line fungerà da primo punto di contatto per qualsiasi reclamo. Qualsiasi lamentela personale di abuso sarà riferita al Dirigente Scolastico.

Denunce di bullismo online saranno trattate in conformità con la legge attuale. Reclami relativi alla protezione dei bambini saranno trattati in conformità alle procedure di protezione dell'infanzia.

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

Alla fine di ogni anno scolastico si effettuerà una valutazione e un monitoraggio in merito alle attività di prevenzione e gestione dei casi da cui scaturirà un eventuale aggiornamento di tale documento. La E-Safety Policy si inserisce all'interno di altre politiche scolastiche, quali la politica di protezione dei minori, la politica anti-bullismo, la politica del benessere degli alunni a scuola.

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

Nell'ambito della revisione della Policy, tutte le informazioni e le revisioni saranno memorizzate per eventuali controlli.

## **1.6 Integrazione della policy con regolamenti esistenti**

Nel Regolamento d'Istituto verrà inserito un apposito allegato estratto dalla Policy che definirà per studenti e personale della scuola l'uso corretto e responsabile delle risorse tecnologiche e di rete (attrezzature hardware e software, Internet ecc.).

# **2. Formazione e curriculum**

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

Il termine competenza si è affermato all'interno del lessico educativo ed anche in Italia è diventato un significativo elemento del processo di riforma del sistema scolastico. Il concetto di

didattica per competenze ha assunto un ruolo centrale in ambito europeo, poiché la loro certificazione offre un terreno comune per la comparazione tra sistemi formativi al di là dei diversi programmi scolastici e pone le basi per la definizione di un modello di cittadinanza europea. Nel 2006 il Parlamento Europeo ha elaborato una Raccomandazione (2006/962/CE), in cui delinea il quadro delle competenze necessarie per il lifelong learning, ovvero competenze necessarie per esercitare pienamente il diritto di cittadinanza nella società. Tra queste competenze è stata inserita anche la competenza digitale. 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 presuppone una solida consapevolezza e conoscenza della natura, del ruolo e delle opportunità delle TIC nel quotidiano: nella vita privata e sociale come anche al lavoro. In ciò rientrano le principali applicazioni informatiche come trattamento di testi, fogli elettronici, banche dati, memorizzazione e gestione delle informazioni oltre a una consapevolezza delle opportunità e dei potenziali rischi di Internet e della comunicazione tramite i supporti elettronici (e-mail, strumenti della rete) per il lavoro, il tempo libero, la condivisione di informazioni e le reti collaborative, l'apprendimento e la ricerca. Le persone dovrebbero anche essere consapevoli di come le TIC possono coadiuvare la creatività e l'innovazione e rendersi conto delle problematiche legate alla validità e all'affidabilità delle informazioni disponibili e dei principi giuridici ed etici che si pongono nell'uso interattivo delle TIC.

Le abilità necessarie comprendono la capacità di cercare, raccogliere e trattare le informazioni e di usarle in modo critico e sistematico, accertandone la pertinenza e distinguendo il reale dal virtuale pur riconoscendone le correlazioni. Le persone dovrebbero anche essere capaci di usare strumenti per produrre, presentare e comprendere informazioni complesse ed essere in grado di accedere ai servizi basati su Internet, farvi ricerche e usarli; dovrebbero, inoltre, anche essere capaci di usare le TIC a sostegno del pensiero critico, della creatività e dell'innovazione.

L'uso delle TIC comporta un'attitudine critica e riflessiva nei confronti delle informazioni disponibili e un uso responsabile dei mezzi di comunicazione interattivi. Anche un interesse a impegnarsi in comunità e reti a fini culturali, sociali e/o professionali serve a rafforzare tale competenza. Nella normativa di riferimento della scuola italiana non possiamo effettivamente parlare dell'introduzione di un curriculum specifico ed unitario dedicato ai linguaggi mediali e alla competenza digitale, tuttavia nelle Indicazioni Nazionali per il curriculum della scuola dell'infanzia e del primo ciclo di istruzione troviamo il riferimento a obiettivi di apprendimento e traguardi di competenze nelle diverse aree disciplinari. La competenza digitale va quindi a configurarsi non come disciplina autonoma, ma come ambito che gli alunni possono sviluppare in maniera trasversale nel complesso delle attività didattiche.

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

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

- migliorare le competenze digitali degli studenti anche attraverso un uso consapevole delle stesse;
- implementare le dotazioni tecnologiche della scuola al fine di migliorare gli strumenti didattici e laboratoriali ivi presenti;
- favorire la formazione dei docenti sull'uso delle nuove tecnologie ai fini dell'innovazione didattica;

- individuare un Animatore Digitale ed un *team* per l'innovazione digitale che supporti ed accompagni adeguatamente l'innovazione didattica, nonché l'attività dell'animatore Digitale;
- partecipare a bandi nazionali ed europei per finanziare le suddette iniziative;

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

- programmare attività e far partecipare gli alunni a laboratori di Coding in occasione della Settimana del codice;
- sviluppare una serie di strategie per valutare e verificare le informazioni prima di accettare l'esattezza;
- essere a conoscenza che l'autore di un sito web / pagina può avere un particolare pregiudizio;
- sapere come restringere o affinare una ricerca;
- capire il comportamento accettabile quando si utilizza un ambiente online, vale a dire, essere educato, non utilizzare comportamenti inappropriati, mantenere le informazioni personali private;
- capire come le fotografie possono essere manipolate e individuare contenuti web in grado di attrarre il tipo sbagliato di attenzione;
- capire perché 'amici' on-line potrebbero non essere chi dicono di essere e di comprendere perché dovrebbero fare attenzione in un ambiente online;
- capire il motivo per cui non dovrebbero inviare o condividere resoconti dettagliati delle loro vite personali e informazioni di contatto;
- capire il motivo per cui non devono pubblicare foto o video di altri senza il loro permesso;
- sapere di non scaricare alcun file - come i file musicali - senza permesso;
- comprendere l'impatto di bullismo online, sexting, grooming e sapere come cercare aiuto se sono in pericolo;
- sapere come segnalare eventuali abusi tra cui il bullismo on-line e come a chiedere aiuto ai docenti, ai genitori, se si verificano problemi quando si utilizzano le tecnologie Internet;
- utilizzare con attenzione Internet per garantire che si adatti alla loro età e supporti gli obiettivi di apprendimento per le aree curriculari specifiche.

## **2.2 Formazione dei docenti sull'utilizzo e l'integrazione delle tic nella didattica**

I docenti della nostra scuola sono dotati di buone competenze digitali, sia certificate che non. In riferimento alla Media Education, che è un ambito di studio, pratica e ricerca che si colloca a metà tra le scienze dell'educazione e quelle della comunicazione e che si concentra sul rapporto tra media e educazione, i docenti manifestano esigenze formative per migliorare le proprie competenze in merito alla:

- educazione ai media (teaching about the media): i media sono l'oggetto dell'intervento educativo, che quindi mira a promuovere una riflessione critica e una sperimentazione creativa, la decodifica e la conoscenza dei messaggi e dei linguaggi mediali;
- educare con i media (teaching with the media): in questo caso i media sono considerati come strumenti attraverso cui realizzare l'intervento formativo, cioè l'utilizzo dei computer, delle LIM o di tablet e smartphone a scuola nella pratica didattica quotidiana.

Si promuoveranno pertanto attività di autoformazione, diffusione di materiali, incontri formativi specifici con relatori interni o esterni, corsi on-line.

## **2.3 Formazione dei docenti sull'utilizzo consapevole e sicuro di internet e delle tecnologie digitali**

Analogamente i docenti manifestano esigenze formative inerenti anche alla dimensione relazionale e affettiva dell'utilizzo delle tecnologie, da trasmettere anche agli alunni, come le modalità per la tutela della privacy, le strategie per il contrasto del fenomeno del cyberbullismo e di altri fenomeni in rete.

Si promuoveranno pertanto, anche in tal caso, attività di autoformazione, diffusione di materiali, incontri formativi specifici con relatori interni o esterni, corsi on-line.

## **2.4 Sensibilizzazione delle famiglie**

La scuola opererà affinché le famiglie siano informate attraverso iniziative specifiche e partecipino come partner educativi nei percorsi di formazione che riguardano gli studenti.

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

- presentare ai genitori, i cui figli si scrivono nel nostro Istituto, il Regolamento d'Istituto;
- pubblicazioni sul sito della scuola;
- offrire incontri di consulenza con esperti;
- fornire informazioni sui siti nazionali di sostegno per i genitori, quali il sito [www.generazioniconnesse.it](http://www.generazioniconnesse.it).

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

### **Introduzione**

L'obiettivo principale della nostra scuola è quello di educare e sensibilizzare gli adolescenti, gli insegnanti e i genitori all'uso sicuro e consapevole di internet.

Si tiene in considerazione il fatto che il curriculum scolastico prevede che gli studenti imparino a trovare materiale, recuperare documenti e scambiare informazioni utilizzando le TIC. Internet, d'altra parte, offre sia agli studenti che agli insegnanti una vasta scelta di risorse diverse e opportunità di scambi culturali con gli studenti di altri paesi. Inoltre, su Internet si possono recuperare risorse per il tempo libero, le attività scolastiche e sociali. La scuola propone agli studenti e agli insegnanti di utilizzare Internet per promuovere l'eccellenza in ambito didattico attraverso la condivisione delle risorse, l'innovazione e la comunicazione. L'accesso ad Internet è un privilegio e un diritto. L'obiettivo principale resta quello di arricchire ed ampliare le attività didattiche, secondo quanto prevede il curriculum scolastico, l'età e la maturità degli studenti.

Le apparecchiature presenti nella Scuola sono un patrimonio comune, quindi, vanno utilizzate con il massimo rispetto. L'utilizzo delle apparecchiature è regolamentato da criteri che puntano a massimizzare la collaborazione collegiale: le prenotazioni, la tracciabilità delle apparecchiature, la segnalazione di malfunzionamenti, sono accorgimenti necessari per evitare disguidi organizzativi, smarrimenti, per rintracciare tramite i docenti la causa di un malfunzionamento. Gli insegnanti sono responsabili delle TIC nell'ambito dell'attività didattica e hanno il compito di responsabilizzare gli alunni per divenire consapevoli dell'importanza della salvaguardia di un bene comune, seguendo le corrette norme di utilizzo.

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

I computer portatili nelle aule accedono ad Internet attraverso rete WIFI. Nel laboratorio informatico e linguistico sono presenti computer fissi che accedono tramite rete LAN. Tutti i computer presenti nella scuola dovranno installare un antivirus. Gli studenti non possono accedere con i loro dispositivi alla rete

internet della scuola. I docenti possono accedere con i loro dispositivi personali alla rete nella scuola, tramite account istruzione. Gli studenti possono accedere ad Internet solo in occasione di attività didattiche che si svolgono nel laboratorio informatico, linguistico o in classe solo su autorizzazione del docente per fini didattici.

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

L'Istituto dispone di una rete con tecnologia senza fili. L'accesso alla rete wireless è regolato da un controller che determina l'accesso degli utenti, docenti e studenti, tramite password. L'ottenimento delle credenziali è riservato a studenti, personale dell'Istituto e ospiti.

I computer portatile destinati alle aule non richiedono una password di accesso per l'accensione. Ogni docente è quindi tenuto ad un controllo della strumentazione in aula poiché l'uso del dispositivo è permesso agli alunni solo su autorizzazione dell'insegnante. Ogni docente accede al registro elettronico attraverso una password personale che non può essere comunicata a terzi, né agli alunni.

### **3.3 E-mail**

Questa scuola non pubblica indirizzi di posta elettronica personali degli alunni o del personale sul sito della scuola.

### **3.4 Sito della scuola**

L'Istituto dispone di un proprio spazio web e di un proprio Dominio:

<http://www.scuolamediabaldassarre.gov.it/>

L'Istituto cura un proprio sito web nello spazio di proprietà. La gestione del sito della scuola e la rispondenza alle normative per quanto concerne i contenuti (accuratezza, appropriatezza, aggiornamento) sono a cura dell'Animatore Digitale e del docente Funzione Strumentale Area Nuove Tecnologie.

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

### **3.5 Protezione dei dati personali**

La scuola "Gen. E. Baldassarre" rispetta la privacy dei propri utenti e si impegna a proteggere i dati personali che gli stessi conferiscono. In generale, l'utente può navigare sul sito web della scuola senza fornire alcun tipo di informazione personale. La raccolta ed il trattamento di dati personali avvengono, quando necessari, in relazione all'esecuzione di servizi richiesti dall'utente, o quando l'utente stesso decide di comunicare i propri dati personali; in tali circostanze, la presente politica della privacy illustra le modalità ed i caratteri di raccolta e trattamento dei dati personali dell'utente. I dati personali forniti dagli utenti vengono trattati in conformità alla normativa vigente.

In caso di raccolta di dati personali, si informerà l'utente sulle finalità della raccolta al momento della stessa, ove necessario, richiederà il consenso dell'utente. La scuola non comunicherà i dati personali dell'utente a terzi senza il consenso dello stesso. Se l'utente decide di fornire alla scuola i propri dati personali, la scuola potrà comunicarli all'interno dell'Istituto od a terzi che prestano servizi alla scuola, solo rispetto a coloro che hanno bisogno di conoscerli in ragione delle proprie mansioni, e, ove necessario, con il permesso dell'utente stesso. La scuola tratta i dati personali dell'utente per le seguenti finalità di carattere generale: per soddisfare le richieste a specifici prodotti o servizi, per personalizzare la visita dell'utente al sito, per aggiornare l'utente sulle ultime novità in relazione ai servizi offerti od altre informazioni che ritiene siano di interesse dell'utente che provengono direttamente dall'Istituto o dai suoi partners, e per comprendere meglio i bisogni dell'utente ed offrire allo stesso servizi migliori. Il trattamento di dati personali dell'utente da parte dell'Istituto per le finalità sopra specificate avviene in conformità alla normativa vigente a tutela dei dati personali.



## **4 Strumentazione personale**

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

Agli studenti è vietato l'utilizzo del cellulare o dei tablet all'interno della scuola, ma essi possono essere utilizzati solo se richiesti dal docente per ragioni prettamente didattiche scolastiche, come previsto dal regolamento BYOD. Gli studenti non possono accedere alla rete attraverso i dispositivi personali se non dietro previa autorizzazione dell'insegnante presente in aula e comunque per ricerche attinenti le attività didattiche.

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

I docenti possono utilizzare cellulari e tablet per motivi didattici mentre è vietato l'uso personale durante l'attività didattica e lavorativa.

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

Il personale della scuola può utilizzare cellulari e tablet per motivi didattici e non a scopo personale durante l'attività didattica o lavorativa.

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

Gli interventi che la scuola dovrà mettere in atto sono tesi a far conoscere e sensibilizzare gli alunni verso un uso responsabile e consapevole della rete, al fine di assicurare loro il rispetto del diritto ad essere tutelati da abusi e violenze da un lato e, allo stesso tempo, suscitare atteggiamenti di rispetto nei confronti degli altri utenti. Le nuove tecnologie si pongono quale strumento attraverso cui sviluppare pratiche di collaborazione tra gli studenti per riconoscere e accettare la diversità e favorire la partecipazione finalizzata alla costruzione dei diversi percorsi formativi a cui sono chiamati tutti gli alunni.

La nostra scuola intraprenderà azioni di coinvolgimento della comunità scolastica in percorsi di prevenzione dei comportamenti a rischio online. I casi rilevati verranno gestiti affrontando il problema sotto diversi punti di vista. In prima luogo si informeranno gli alunni sulle conseguenze relative al fenomeno emerso, dall'altro si cercherà di aiutare l'alunno/a coinvolto e vittima creando situazioni di dialogo che consentano di far emergere gli aspetti di criticità per i quali attraverso un confronto si potrà intervenire.

I docenti dovranno predisporre delle rilevazioni e qualora si rendano conto che si trovano di fronte a situazioni di criticità dovranno rivolgersi al responsabile che avvierà le procedure con le istituzioni preposte nonché la segnalazione alla Dirigenza Scolastica. Tali rilevazioni avvengono secondo i protocolli suggeriti dalla piattaforma messa a disposizione da "Generazioni Connesse", come da schemi allegati. Inoltre, ci si potrà avvalere del servizio **Hotline** che si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la rete. I due servizi messi a disposizione dal **Safer Internet Center** sono il "**Clicca e Segnala**" di **Telefono Azzurro** e "**STOP-IT**" di **Save the Children**. Una volta ricevuta la segnalazione, gli operatori procederanno a coinvolgere le autorità competenti in materia.

### **5.1 Prevenzione**

Principi generali:

1. Internet favorisce la libertà d'espressione e, quando si entra a far parte di una community o di un servizio in cui interagiscono più utenti, vanno considerati abusi meritevoli di segnalazione solo i contenuti palesemente impropri o illeciti e non tutti quei contenuti con cui semplicemente non si è d'accordo.
2. Quando si inizia a navigare tra i servizi dei Social Network e applicazioni web del tipo YouTube, Facebook, Netlog, etc., bisogna informarsi subito su quali sono i diritti e i doveri dell'utente, leggendo il regolamento, tenendosi aggiornati, esplorando i siti informativi e istituzionali che affrontano queste tematiche.
3. Se si condividono informazioni personali, bisogna farlo scegliendo con cura che cosa rendere pubblico e cosa rendere privato. È indispensabile scegliere con attenzione i contatti con cui accrescere la propria rete e i gruppi a cui aderire, proteggendo la propria identità digitale con password complesse e usando una domanda di recupero password dalla risposta non banale.
4. Se si condividono elementi multimediali o informazioni che riguardano più persone è necessario avere il permesso di ciascun utente coinvolto prima di effettuare la pubblicazione. Ad esempio, non bisogna pubblicare su YouTube video girati di nascosto e nei quali siano presenti persone filmate senza il loro consenso.
5. Bisogna contribuire a rendere il Web un luogo sicuro, pertanto ogni volta che un utente commette involontariamente un abuso o un errore, pubblicando del materiale illecito, non idoneo o offensivo, bisogna contattarlo e fornire le spiegazioni relative alle regole, diffondendo così i principi della sicurezza.
6. Ogni abuso subito o rilevato nella navigazione, deve essere segnalato tramite i canali e gli strumenti offerti dal servizio che ospita tali contenuti, indicando in modo semplice i riferimenti per ottenere tempestivamente la rimozione del contenuto (abuso, data, ora, utenti e servizio coinvolti). Tutti i social network garantiscono la possibilità di segnalare materiale inopportuno mediante semplici operazioni da compiere direttamente sul sito. Prima di trasformare un incidente o una "bravata" in una denuncia alle autorità competenti, è opportuno avvalersi della modalità di segnalazione che non obbliga le parti in causa a conseguenze penali e giudiziarie che possono durare anni.

**Scuola e Famiglia** possono essere determinanti nella diffusione di un atteggiamento mentale e culturale che consideri la diversità come una ricchezza e che educi all'accettazione, alla consapevolezza dell'altro, al senso della comunità e della responsabilità collettiva. Occorre, pertanto, rafforzare e valorizzare il Patto di Corresponsabilità educativa: la scuola è chiamata ad adottare misure atte a prevenire e contrastare ogni forma di violenza e di prevaricazione; la famiglia è chiamata a collaborare, non solo educando i propri figli ma anche vigilando sui loro comportamenti.

Per definire una strategia ottimale di prevenzione e di contrasto, le esperienze acquisite e le conoscenze prodotte vanno contestualizzate alla luce dei cambiamenti, che hanno profondamente modificato la società, sul piano etico, sociale e culturale, e ciò comporta una valutazione ponderata delle procedure adottate per riadattarle in ragione di nuove variabili, assicurandone in tal modo l'efficacia.

La forma online del bullismo ha, tuttavia, alcuni elementi di pericolosità peculiari, di cui occorre avere consapevolezza.

1. Il cyberbullismo è *pervasivo*: il cyberbullo può raggiungere la sua vittima in qualsiasi momento e in qualsiasi luogo. La possibilità di avere smartphone sempre accesi e spesso connessi ad Internet permette al cyberbullo di aggredire la sua vittima ogni volta che lo desidera.
2. Il cyberbullismo è un *fenomeno persistente*: il materiale diffamatorio pubblicato su Internet può rimanere disponibile online anche per molto tempo;
3. Spettatori e cyberbulli sono *potenzialmente infiniti*: le persone che possono assistere a episodi di cyberbullismo sono potenzialmente illimitate e molti soggetti possono diventare complici dei cyberbulli anche solo condividendo o promuovendo l'episodio di cyberbullismo, che finisce per replicarsi (ad esempio sulle bacheche dei profili che i ragazzi hanno sui social network) in modo incontrollabile.

## 5.2 Azioni

Premesso, sul piano generale, che l'utilizzo da parte degli alunni di tutte le apparecchiature tecnologiche di informazione e comunicazione viene rigorosamente disciplinato da quanto disposto dal Regolamento d'Istituto e, in modo precipuo, dal Regolamento BYOD, si individuano, da parte di tutti i soggetti coinvolti nel processo educativo, le seguenti azioni di prevenzione.

La scuola avrà cura di porre attenzione alla rilevazione di rischi connessi alla navigazione sul web.

In modo particolare:

- Cyberbullismo;
- Adescamento online;
- Sexting;
- Pornografia;
- Pedopornografia;
- Gioco d'azzardo o Gambling;
- Dipendenza da Internet
- Esposizione a contenuti dannosi o inadeguati.

In particolare i **docenti si impegnano a :**

- organizzare le attività didattiche e formative che prevedano l'utilizzo delle TIC da parte degli alunni (LIM presenti nelle classi, PC nei laboratori , PC portatili, tablet, notebook) in modo che esse siano adoperate sempre sotto la supervisione del docente;
- accompagnare gli alunni nella navigazione in Rete, coinvolgendoli nell'esplorazione delle opportunità e dei rischi, con idonee attività finalizzate a tale scopo;
- riaffermare sistematicamente l'importanza della riservatezza sui propri dati personali;
- approfondire, con attività mirate in classe, la conoscenza del fenomeno del bullismo e del cyberbullismo;
- creare degli spazi in cui gli alunni si possano confrontare su questo tema, utilizzando come spunti di riflessione documenti filmati, canzoni, materiali prodotti da altri alunni, presentazioni multimediali, testi sull'argomento ed ogni altro materiale utile;
- vigilare con attenzione, essere pronti a cogliere eventuali segnali di disagio che emergano da possibili situazioni di abuso e manifestare costante disponibilità all'ascolto e al dialogo;
- collaborare con l'azione condotta dal Dirigente Scolastico, dai referenti d'Istituto, dall'Animatore Digitale e dal team digitale, i quali progettano e coordinano le diverse attività di prevenzione e formazione sul fenomeno del cyberbullismo a favore di tutta la comunità scolastica;
- confrontarsi con gli altri insegnanti della classe, della scuola o con esperti del territorio;
- fare ricorso, per ogni necessità informativa o infomativa, agli strumenti disponibili online sulla piattaforma "Generazioni connesse" ([www.generazioniconnesse.it](http://www.generazioniconnesse.it)).

### 5.3 Rilevazione e gestione dei casi

Intervenire in situazioni di cyberbullismo non è mai semplice: spesso si pensa di non sapere esattamente cosa fare e si ha timore di essere inadeguati. Per tale motivo la scuola si impegna ad individuare alcuni strumenti che potranno agevolare l'intera comunità scolastica nel decidere come intervenire e nel tenere traccia di ciò che è avvenuto rispetto ai comportamenti degli alunni online e di come è stato gestito il problema.

L'obiettivo a lungo termine che la comunità scolastica si propone è quello di creare strumenti condivisi per orientare in modo sempre più efficace le azioni di contrasto ad episodi che, nel tempo, potrebbero ripetersi.

**Per la rilevazione** dei casi, la scuola punta, in primo luogo, sulla centralità del dialogo educativo, invitando gli alunni a segnalare ai docenti, e in particolar modo al Coordinatore del Consiglio di Classe, eventuali casi di abusi. Quale utile elemento integrativo a tale azione, la scuola mette a disposizione degli studenti - in accordo con i progetti "Generazioni Connesse" e "Il nodo blu nelle scuole pugliesi" - una cassetta postale per la raccolta, in forma anonima e riservata, di bigliettini per segnalare eventuali casi di bullismo e cyberbullismo, all'interno dell'Istituto. I messaggi vengono raccolti, ottemperando alle norme

sulla privacy, solo ed esclusivamente dal Dirigente Scolastico e dai docenti referenti del progetto e trattati con la massima riservatezza per monitorare il fenomeno e predisporre eventuali interventi sul piano educativo.

**Per una efficace gestione** dei casi la scuola si riserva di utilizzare lo schema messo a disposizione sul sito [www.generazioniconnesse.it](http://www.generazioniconnesse.it) (Allegato n. 1).

I docenti sono tenuti a segnalare gli alunni che non rispettano le corrette modalità di accesso e di uso di Internet e delle TIC a scuola. Nei casi di fenomeni di cyberbullismo o di violazione della privacy o di mancato rispetto delle regole di sicurezza durante la navigazione, gli alunni saranno sanzionati dall'organo di garanzia costituito nella scuola con procedimenti disciplinari proporzionali all'infrazione commessa.

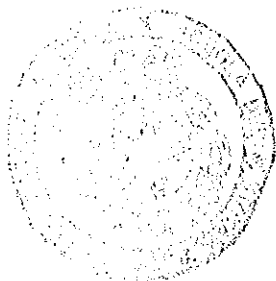
**Per poter tenere traccia** di ciò che è avvenuto rispetto ai comportamenti degli alunni online e di come è stato gestito il problema, la scuola si riserva di utilizzare un "Diario di Bordo", secondo il modello messo a disposizione sul sito [www.generazioniconnesse.it](http://www.generazioniconnesse.it)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

## 6. Annessi

Allegato 1 - Schema per la gestione dei casi

Allegato 2 - Diario di bordo per la registrazione di casi

Allegato 3 - Modulo di segnalazione dei casi



IL DIRIGENTE SCOLASTICO

Prof.ssa Gabriella CATAACCHIO

A handwritten signature in black ink, appearing to read "G. Cataacchio", written over the printed name.