Ministero dell'Istruzione e del Merito
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
ISTITUTO COMPRENSIVO STATALE
"Parco degli Acquedotti"
Cod. Mecc. RMIC8GG001 - C.F. 97712420583 – C.U.: UFMEP2
Sede Legale: Via Lemonia, 226 - 00174 Roma ☎ 06 95955242
www.icparcodegliacquedotti.edu.it
✉rmic8gg001@istruzione.it - ✉rmic8gg001@pec.istruzione.it

E-Safety Policy

Documento programmatico per la sicurezza in rete e l'integrazione delle TIC nella didattica,

Anno scolastico 2023/24

INDICE RAGIONATO
E-Safety Policy

1. Introduzione

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

2. Formazione e Curricolo

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

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

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

4. Strumentazione personale

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

5. Prevenzione, rilevazione e gestione dei casi

Prevenzione

- Rischi
- Azioni

Rilevazione

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

Gestione dei casi

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

Annessi (da prodursi a cura della scuola)

1. Procedure operative per la gestione delle infrazioni alla Policy.
2. Procedure operative per la protezione dei dati personali.
3. Procedure operative per la rilevazione, il monitoraggio e la gestione delle segnalazioni.
4. Procedure operative per la gestione dei casi.
5. Protocolli siglati con le forze dell'ordine e i servizi del territorio per la gestione condivisa dei casi.

1. Introduzione

1.1 Scopo della Policy

L'utilizzo sempre più diffuso delle TIC (Tecnologie dell'Informazione e della Comunicazione) all'interno degli ambienti scolastici da parte di tutti i componenti della comunità educativa pone l'accento sulla necessità di educare ad un loro uso corretto e responsabile.
In particolare l'intento della scuola è quello di promuovere l'uso consapevole e critico da parte degli alunni delle tecnologie digitali e di internet, di far acquisire loro procedure e competenze "tecniche" ma anche corrette norme comportamentali, di prevenire, ovvero rilevare e fronteggiare, le problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso, delle tecnologie digitali. Gli utenti, siano essi maggiorenni o minori, 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.

L'E–Safety dell' Istituto Comprensivo Parco degli Acquedotti, insieme agli altri regolamenti d'Istituto e alle politiche relative ai comportamenti degli alunni definisce pertanto:

- misure di prevenzione e di gestione di situazioni problematiche relative all'uso delle tecnologie digitali;

- misure atte a facilitare e promuovere l'utilizzo positivo delle TIC nella didattica e negli ambienti scolastici.

1.2 Ruoli e Responsabilità.

L'Istituto Comprensivo Parco degli Acquedotti ha costituito un gruppo di lavoro, formato dall'Animatore digitale, dal Team digitale, dai Referenti per il Bullismo e il Cyberbullismo, che si occupa della stesura e del monitoraggio della E – Policy.
Il seguente documento definisce in modo chiaro i ruoli e le responsabilità di ogni membro della comunità educante.

- ***Dirigente Scolastico***

Il ruolo del Dirigente scolastico nel promuovere l'uso consentito delle tecnologie e di internet include i seguenti compiti:

- Garantire il rispetto della E-policy d'Istituto.

- Garantire la sicurezza (tra cui la sicurezza on-line) dei membri della comunità scolastica.
- Garantire l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line.
- Essere a conoscenza delle procedure per la prevenzione, rilevazione e gestione di strategie utili per individuare casi di rischio nell'utilizzo delle TIC a scuola.
- Garantire che tutti gli insegnanti ricevano una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze, un utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della comunicazione (TIC).
- Comprendere e 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.
- Ricevere relazioni periodiche di monitoraggio dai Referenti del bullismo e del cyber bullismo, dall'Animatore digitale e /o dal Team digitale. Dall'a.s. 2023/2024, il Kit Didattico di Generazioni Connesse fornisce inoltre articolate e pertinenti linee guida per un percorso formativo concretamente volto a sottolineare l'importanza di creare una rete educativa sempre più ampia e consapevoli per l'uso corretto delle tecnologie digitali da parte degli alunni di ogni ordine e grado.

-***Animatore digitale***

Il ruolo dell'Animatore digitale nel promuovere l'uso consentito delle tecnologie e di internet implica i seguenti compiti:

- Coordinare e mantenere contatti con il Team digitale, con il Referente del bullismo e del cyberbullismo, con le autorità e gli enti esperti.
- Relazionare periodicamente il lavoro del gruppo con il Dirigente Scolastico.
- 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;
- 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;
- Assicurare che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate e curare la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti.
- Coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti la "scuola digitale".
- Cura dei rapporti con l'assistenza tecnico-informatica per definire le misure di sicurezza informatica più opportune;

- ***Team digitale***

Il ruolo del Team digitale nel promuovere l'uso consentito delle tecnologie e di internet implica i seguenti compiti:

- Definire e revisionare le politiche e i documenti di E–Safety.
- Promuovere la consapevolezza e l'impegno, per la salvaguardia relativa alle tecnologie, di tutta la comunità educante.
- Diffondere la conoscenza delle procedure per la prevenzione, rilevazione e gestione di strategie utili per individuare casi di rischio nell'utilizzo delle TIC a scuola.
- Assicurare che nel curricolo scolastico vengano inseriti i diversi aspetti della sicurezza in internet.
- Monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie

digitali e di internet a scuola (condivisione di dati personali, accesso a materiali illegali e/o inadeguati, cyber – bullismo, ecc. …).

- ***Referente bullismo e cyberbullismo***

Il ruolo del Referente del bullismo e cyberbullismo (Legge n. 71 del 29/05/2017, Disposizioni a tutela dei minori per la prevenzione del fenomeno del cyberbullismo) nel promuovere l'uso consentito delle tecnologie e di internet implica i seguenti compiti:

- Elaborare strumenti conoscitivi del fenomeno.
- Partecipare alla stesura/revisione annuale della Policy di E-Safety e a curarne la massima diffusione all'interno di tutta la comunità scolastica.
- Prendere atto dei risultati dei monitoraggi in itinere e finali per il controllo delle procedure interne per la sicurezza informatica.
- Verificare ed implementare, alla fine dell'anno scolastico, la validità della Policy di E-Safety.
- . Proporre degli eventi per presentare l'e-policy alle famiglie e agli studenti.
- . Raccogliere tutte le segnalazioni effettuate dai docenti.
- Offrire consulenza e coordinamento relativamente alle procedure da seguire per una corretta gestione dei casi.
- Informare e collaborare costantemente con il D.S. per il monitoraggio e l'implementazione della Policy di E-Safety.
- Collaborare con l'animatore digitale per diffondere materiale informativo, per prevenire eventi di bullismo e cyberbullismo, che possano coinvolgere gli alunni dell'istituto e per effettuare eventuali indagini digitali.
- Ascoltare e aiutare gli alunni per ridurre e prevenire fenomeni di illegalità e inciviltà o chi si trova in difficoltà perché oggetto di prevaricazioni online.
- Intervenire nei confronti di chi fa un uso inadeguato della rete e dei cellulari, ascoltando eventuali problemi e fornendo consigli.
- Sensibilizzare, dare informazioni agli alunni e alle famiglie su quelli che sono i rischi della rete, comunicandogli le azioni che la scuola mette in atto in caso di fenomeni di bullismo e cyberbullismo.
- Informare gli insegnanti della eventuale presenza di casi di bullismo e cyberbullismo.
- Convocare, sentito il parere del Dirigente Scolastico, gli interessati di atti di bullismo e cyberbullismo per adottare misure di assistenza alla vittima e sanzioni, in base alla gravità del fatto, e percorsi rieducativi per l'autore.
- Promuovere e pubblicizzare le iniziative di formazione rivolte agli alunni, ai genitori, ai docenti e al personale ATA dell'Istituto comprensivo.
- Coordinare le iniziative di prevenzione e di contrasto del bullismo e del cyberbullismo, anche in collaborazione con le Forze di Polizia di Stato, associazioni e centri di aggregazione giovanili presenti nel territorio.
- Coordinare e curare il monitoraggio delle azioni intraprese per combattere i fenomeni di bullismo e cyberbullismo.
- Mettere a disposizione la normativa vigente e i materiali di approfondimento.

- ***Direttore dei servizi generali e amministrativi***

Il ruolo del direttore dei servizi generali e amministrativi include i seguenti compiti:

- Assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnologica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni;
- Garantire il funzionamento dei diversi canali di comunicazione dell'Istituto all'interno della comunità scolastica e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni nell'ambito dell'utilizzo delle TIC.

- ***Lo staff***

Il ruolo dello Staff implica i seguenti compiti:

- Promuovere le politiche di E–Safety dell'Istituto.
- Essere consapevole dei problemi di sicurezza correlati all'utilizzo delle nuove tecnologie digitali, monitorandone l'utilizzo e applicando le vigenti politiche scolastiche in materia.
- Segnalare ai Referenti del bullismo e del cyberbullismo ogni tipo di abuso o di problema.
- Favorire comportamenti responsabili e sicuri nell'utilizzo della tecnologia.

- ***Docenti***

Il ruolo del personale docente e di ogni figura educativa che lo affianca implica i seguenti compiti:

- Informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento.
- Garantire che le modalità di utilizzo corretto e sicuro delle TIC e di internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi.
- Garantire che gli alunni capiscano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di Internet.
- 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 (privacy, copyright…).
- Garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali.
- Assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente.
- Controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito).
- Nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei.
- 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.
- Segnalare al Dirigente scolastico, 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

- ***Tecnico esterno***

Il ruolo del tecnico esterno implica i seguenti compiti:

- Eseguire una manutenzione periodica dell'infrastruttura tecnologica dell'Istituto.
- Fare un controllo periodico al sistema di sicurezza dei dati (firewall, filtri, server per il controllo degli account…).

- ***Studenti***

Il ruolo degli studenti implica i seguenti compiti:

- Aderire all'E–Safety dell'Istituto in relazione al proprio grado di maturità e di apprendimento, per un utilizzo responsabile e corretto delle TIC.
- Avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali, ma anche della necessità di evitare il plagio e rispettare i diritti d'autore.
- Comprendere l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi e di segnalare gli abusi.
- Adottare condotte rispettose degli altri anche quando si comunica in rete.
- Esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di

internet ai docenti, al Referente del bullismo e cyber-bullismo, al Dirigente scolastico e ai genitori.
- Rispettare le indicazioni date dalla scuola sull' utilizzo dei devices.

- ***Genitori***

Il ruolo dei genitori implica i seguenti compiti:

- Leggere, comprendere, aderire all'E–Safety dell'Istituto per un utilizzo responsabile e corretto delle TIC da parte dei propri figli.
- Sostenere la linea di condotta dell'Istituto nei confronti dell'utilizzo delle tecnologie dell'informazione e delle comunicazioni nella didattica.
- Concordare con i docenti e con il Referente del bullismo e del cyberbullismo linee di intervento coerenti e di carattere educativo in relazione all'utilizzo delle TIC soprattutto in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitale o della rete.
- Seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dalla scuola, in particolare controllare l'utilizzo del pc e di internet;
- 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
- Partecipare alle iniziative di formazione proposte dall'istituto in materia di sicurezza di rete.

1.3 Condivisione e comunicazione della Policy all'intera comunità scolastica

Vista l'importanza di un corretto uso delle TIC e della rete internet e per diffondere la consapevolezza delle norme di comportamento e delle conseguenti sanzioni in caso di cattivo utilizzo, l'E–Safety Policy verrà presentata e condivisa con l'intera comunità scolastica avvalendosi di diversi mezzi e con l'aiuto di tutte le componenti dell'Istituto.

- ***Condividere e comunicare la politica di E– Safety agli alunni***

- Presentazione della E–Safety alle classi quarte e quinte della scuola Primaria e a tutte le classi della scuola Secondaria di Primo grado.
- Affissione dell'elenco delle regole per la sicurezza on-line in tutte le aule e laboratori con accesso ad internet.
- Riflessione sugli aspetti della sicurezza in rete per i quali gli alunni risultano più esposti (cyber bullismo, grooming, sexting, ecc.).
- Formazione sull'argomento in classe nelle ore curricolari/extracurricolari, con i docenti e/o con esperti esterni.

- ***Condividere e comunicare la politica di E–Safety ai genitori***

- Pubblicazione della versione integrale della E–Safety sul sito web dell'Istituto.
- Collaborazione tra scuola e famiglia sulla condivisione di regole comuni sulla sicurezza nell'uso delle TIC e di internet.
- Formazione sull'argomento.
- Supporto alle famiglie da parte dell'Animatore digitale e dei Referenti del bullismo e cyber bullismo per l'individuazione di strumenti adeguati a garantire la navigazione sicura anche a casa.

1.4 *Gestione delle infrazioni alla Policy.*

- ***Alunni***

Gli interventi correttivi previsti per gli alunni vanno 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 proporzionati all'età e alla gravità del comportamento, quali:

- il richiamo verbale;
- il richiamo scritto con annotazione sul diario e il registro elettronico;
- il ritiro del dispositivo da parte del docente e la sua riconsegna al termine delle lezioni;
- la convocazione dei genitori da parte degli insegnanti;
- la convocazione dei genitori da parte del Dirigente scolastico.

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.
La valutazione spetta al Dirigente Scolastico e all'equipe pedagogica/Consiglio di classe. Rimangono, inoltre, applicabili ulteriori sanzioni disciplinari e azioni civili per danni, nonché l'eventuale denuncia all'autorità giudiziaria qualora la violazione si configuri come reato.

- ***Personale scolastico***

Tutto il personale scolastico e in particolare i docenti possono incorrere in potenziali infrazioni se utilizzano in modo improprio e scorretto le tecnologie digitali o Internet.
Per evitare ciò devono:

- utilizzare le tecnologie e i servizi della scuola solo e unicamente per attività connesse all'insegnamento o ad attività inerenti al profilo professionale.
- Comunicare elettronicamente con i genitori e gli alunni in modo compatibile con il ruolo professionale.
- Porre particolare attenzione al rispetto del trattamento dei dati sensibili degli alunni come previsto dalle norme relative alla privacy.
- Essere ligi nella conservazione delle password assegnate, al fine di evitare il loro utilizzo improprio da parte di terze persone.
- Curare la formazione degli alunni sull'utilizzo corretto e responsabile delle TIC.
- Vigilare durante l'utilizzo delle TIC da parte degli alunni e segnalare situazioni critiche al Dirigente scolastico e ai preposti.

Il Dirigente scolastico può controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a internet,, procedere alla cancellazione di materiali inadeguati o non autorizzati dal sistema informatico della scuola, conservando una copia per eventuali successivi accertamenti.
I provvedimenti disciplinari e le sanzioni sono quelle previste dalla legge e dai contratti di lavoro.

- ***Genitori***

La collaborazione tra scuola e famiglia è fondamentale per aiutare gli alunni a utilizzare in modo corretto e responsabile le TIC e internet.
In particolare i genitori a casa dovrebbero evitare alcuni comportamenti che possano favorire un uso

scorretto delle tecnologie come:

- una posizione del computer in una stanza o in un posto non visibile a tutti quando è utilizzato dal proprio figlio;
- una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'utilizzo del cellulare o dello smartphone;
- un utilizzo del pc, del cellulare, dello smartphone o del tablet in comune con gli adulti che possono conservare in memoria materiali non idonei;

In caso di infrazioni, i genitori possono essere convocati a scuola per concordare misure educative oppure essere sanzionati a norma di legge in base alla gravità dei comportamenti tenuti dai propri figli.

M***onitoraggio 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 Dirigente scolastico con la collaborazione dell'Animatore digitale, dei Referenti del bullismo e cyberbullismo e dei docenti delle classi. Sarà finalizzato alla rilevazione dell'uso sicuro e responsabile delle tecnologie digitali e di internet al fine di valutare l'impatto della policy e la necessità di eventuali miglioramenti.

1.6 Integrazione della Policy con Regolamenti esistenti

La presente E-Safety si integra pienamente con obiettivi e contenuti dei seguenti documenti, che specificano il contesto di attuazione delle politiche dell'Istituto comprensivo per un uso efficace e consapevole del digitale nella didattica:

- PTOF, e il curricolo di Educazione Civica.
- Regolamento d'Istituto.
- Il patto di corresponsabilità.
- Regolamento sull'uso di dispositivi elettronici da parte degli alunni (linee guida)

In applicazione:

✔ "Linee di orientamento Contro il bullismo e il cyberbullismo" (MIUR – 13 Aprile 2015).
✔ "Piano Nazionale per la prevenzione del bullismo e del cyberbullismo a scuola (MIUR 2016/2017).
✔ "Legge n. 71 del 29/05/2017, Disposizioni a tutela dei minori per la prevenzione del fenomeno del cyberbullismo".

2. Formazione e Curricolo

2.1 Curricolo sulle competenze digitali per gli studenti.

Inserita nelle otto Competenze chiave di cittadinanza attiva, indicate dal Consiglio di Lisbona del 2000, "la **Competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'Informazione (TSI) 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".**
Il Curricolo della scuola del primo ciclo di istruzione sulle competenze digitali per gli alunni è trasversale alle discipline previste dalle Indicazioni Nazionali del 2012. Si ritrovano abilità e conoscenze che fanno capo alla competenza digitale in tutte le discipline e tutte concorrono a

costruirla. La competenza digitale fa riferimento alla capacità di comprendere e sfruttare l'effettivo potenziale delle tecnologie in ottica di costruzione, di conoscenza e di promozione della partecipazione e dell'inclusione; il rapporto con le tecnologie digitali guarda così a forme di uso consapevole, critico e creativo. Il Piano 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.
Nell'ambito del PNSD, questo Istituto si propone un programma di progressiva educazione alla sicurezza online, come parte del curricolo scolastico e si impegna a sviluppare una serie di competenze e comportamenti adeguati all'età degli alunni e alla loro esperienza. La scuola ha già proposto e continuerà ad offrire laboratori di coding. Ha iniziato a sviluppare una serie di strategie per aiutare gli alunni ad adoperare un comportamento corretto quando si utilizza un ambiente online e a non inviare o condividere materiali inadeguati.
Ha organizzato incontri per far comprendere l'impatto del bullismo online, sexting, grooming e sapere come cercare aiuto se si presentano situazioni di pericolo. Si sta, inoltre, adoperando per garantire che Internet si adatti all'età degli alunni e supporti gli obiettivi di apprendimento per le aree curricolari specifiche.

COMPETENZA CHIAVE EUROPEA: COMPETENZA DIGITALE - DISCIPLINE DI RIFERIMENTO: tutte

FINE CLASSE TERZA SCUOLA PRIMARIA

COMPETENZE SPECIFICHE	**ABILITA'**	**CONOSCENZE**
Utilizzare le più comuni tecnologie dell'informazione e della comunicazione, individuando le soluzioni potenzialmente utili ad un dato contesto applicativo.	Utilizzare il PC, con la supervisione dell'insegnante, per scrivere, compilare tabelle e disegnare. Utilizzare alcune funzioni principali, come creare un file, caricare immagini, salvare il file.	Uso di applicativi di base per produzione testi, elaborazione grafica e sviluppo,del pensiero computazionale. Funzionamento elementare del PC.
Avviare ad una prima consapevolezza delle potenzialità dei limiti e dei rischi dell'uso delle tecnologie dell'informazione e della comunicazione.	Individuare alcuni rischi fisici nell'uso di apparecchiature elettriche ed elettroniche e ipotizzare soluzioni preventive.	Rischi fisici nell'utilizzo di apparecchi elettrici ed elettronici. Rischi nell'utilizzo della rete con PC.
	Individuare alcuni rischi nell'utilizzo della rete Internet e ipotizzare alcune semplici soluzioni preventive.	

FINE SCUOLA PRIMARIA

COMPETENZE SPECIFICHE	**ABILITA'**	**CONOSCENZE**

Utilizzare le più comuni tecnologie dell'informazione e della comunicazione, individuando le soluzioni potenzialmente utili a un dato contesto applicativo.	Utilizzare il PC, alcune periferiche e programmi applicativi. Utilizzare semplici materiali digitali per l'apprendimento. Avviare alla conoscenza della Rete per scopi d'informazione, comunicazione, ricerca e svago.	I principali dispositivi informatici d'input e output. Uso di applicativi differenziati per produzione ed elaborazione testi, grafica e sviluppo del pensiero computazionale Semplici procedure di utilizzo di Internet per ottenere dati, fare ricerche, comunicare.
Avviare una prima consapevolezza delle potenzialità, dei limiti e dei rischi dell'uso delle tecnologie dell'informazione e della comunicazione.	Individuare rischi fisici nell'utilizzo delle apparecchiature elettriche ed elettroniche e i possibili comportamenti preventivi. Individuare i rischi nell'utilizzo della rete Internet e individuare alcuni comportamenti preventivi e correttivi.	Rischi fisici nell'utilizzo di apparecchi elettrici ed elettronici Rischi nell'utilizzo della rete con

FINE SCUOLA SECONDARIA DI PRIMO GRADO

COMPETENZE SPECIFICHE	**ABILITA'**	**CONOSCENZE**
Utilizzare con dimestichezza le più comuni tecnologie dell'informazione e della comunicazione, individuando le soluzioni potenzialmente utili a un dato contesto applicativo, a partire dall'attività di studio.	Utilizzare strumenti informatici e di comunicazione per elaborare dati, testi e immagini e produrre documenti in diverse situazioni. Conoscere gli elementi basilari che compongono un computer e le relazioni essenziali fra di essi. Collegare (Mettere in relazione) le modalità di funzionamento dei dispositivi elettronici con le conoscenze scientifiche e tecniche acquisite. Utilizzare materiali digitali per l'apprendimento. Utilizzare il PC, periferiche e programmi applicativi Utilizzare la rete per scopi d'informazione, comunicazione, ricerca e svago.	I dispositivi informatici d'input e output Il sistema operativo e i più comuni software applicativi, con particolare riferimento all'office automazioni e ai prodotti multimediali anche Open source. Procedure per la produzione di testi, ipertesti, presentazioni e utilizzo dei fogli di calcolo. Procedure di utilizzo di reti informatiche per ottenere dati, fare ricerche, comunicare. Caratteristiche e potenzialità tecnologiche degli strumenti d'uso più comuni.

Essere consapevole delle potenzialità, dei limiti e dei rischi dell'uso delle tecnologie dell'informazione e della comunicazione, con particolare riferimento al contesto in cui vengono applicate. Avere la piena consapevolezza dei rischi della navigazione non sicura attraverso un'adeguata formazione svolta dai docenti, soprattutto nell'ambito dell'Educazione civica e della Cittadinanza digitale - la Netiquette, il Manifesto delle parole non ostili; conoscenza della legge sul cyberbullismo.	Riconoscere potenzialità e rischi connessi all'uso delle tecnologie più comuni, anche informatiche. Essere consapevoli dei rischi dell'adescamento in rete, e della necessità di tutelare i propri dati sensibili.	Procedure di utilizzo sicuro e legale di reti informatiche per ottenere dati e comunicare (motori di ricerca, sistemi di comunicazione mobile, email, chat, social network, protezione degli account, download, diritto d'autore, ecc.). Fonti di pericolo e procedure di sicurezza.

LIVELLI DI PADRONANZA	
LIVELLO 1	Sotto la diretta supervisione dell'insegnante identifica, denomina e conosce le funzioni fondamentali di base dello strumento. Con la supervisione dell'insegnante, utilizza i principali componenti, in particolare la tastiera. Comprende e produce semplici frasi associandole ad immagini date..
LIVELLO 2	Sotto la diretta supervisione dell'insegnante e con sue istruzioni, scrive un semplice testo al computer e lo salva. Utilizza la rete solo con la diretta supervisione dell'adulto per cercare informazioni.
LIVELLO 3 ***atteso a partire dalla fine della scuola primaria***	Scrive, revisiona e archivia in modo autonomo testi scritti con il PC. Costruisce tabelle di dati con la supervisione dell'insegnante. Accede alla rete con la supervisione dell'insegnante per ricavare informazioni. Conosce e descrive alcuni rischi della navigazione in rete e dell'uso del cellulare e adotta i comportamenti preventivi.

LIVELLO 4 ***atteso nella scuola secondaria di primo grado***	Scrive, revisiona e archivia in modo autonomo testi scritti con il PC; è in grado di modificarli, inserendo immagini, disegni, tabelle. Costruisce tabelle di dati; utilizza fogli elettronici per semplici elaborazioni di dati e calcoli. Utilizza la posta elettronica e accede alla rete con la supervisione dell'insegnante per ricavare informazioni e per collocarne di proprie. Conosce e descrive i rischi della navigazione in rete e dell'uso del cellulare e adotta i comportamenti preventivi.

LIVELLO 5 ***Atteso alla fine della scuola secondaria di primo grado***	Utilizza in autonomia programmi di videoscrittura, fogli di calcolo, presentazioni per elaborare testi, comunicare, eseguire compiti e risolvere problemi. Sa utilizzare la rete per reperire informazioni, con la supervisione dell'insegnante; organizza le informazioni in file, schemi, tabelle, grafici; collega file differenti. Confronta le informazioni reperite in rete anche con altre fonti documentali, testimoniali, bibliografiche. Comunica autonomamente attraverso la posta elettronica. Rispetta le regole della netiquette nella navigazione in rete e sa riconoscere i principali pericoli della rete (spam, falsi messaggi di posta, richieste di dati personali, fake news, ecc.), contenuti pericolosi o fraudolenti, evitandoli.

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 di distretto e di ambito; 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 tecnologica e degli ambienti di apprendimento. Il percorso di formazione in itinere prevede:

- Autoaggiornamento.
- Formazione personale e /o collettiva organizzate dall'Animatore digitale e dal Team digitale.
- Formazione dei docenti all'utilizzo del registro elettronico e dello scrutinio elettronico.
- Somministrazione di un questionario rivolto ai docenti per la rilevazione dei "bisogni formativi".
- Partecipazione alle iniziative promosse dall'Amministrazione centrale e dalle scuole in rete di distretto e di ambito.
- Corsi on-line.

2.3 Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali

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.

2.4 Sensibilizzazione delle famiglie

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.
Sul sito scolastico in itinere 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 possibile e consentito esclusivamente per la didattica, per l'utilizzo del Registro Elettronico e per la comunicazione scolastica. Sarà schermato da filtri (firewall) che impediscono il collegamento a siti appartenenti a black list consentendo il collegamento solo a siti idonei alla didattica. Sui pc client dei laboratori e delle aule sarà impostato il controllo genitori, per limitare l'accesso ai giochi, per disciplinare l'orario di utilizzo delle postazioni.
Tutti gli operatori connessi ad internet devono rispettare le predette norme e la legislazione vigente applicata in materia. Gli utenti si impegnano a non consultare deliberatamente, conservare o diffondere documenti che possono ledere la dignità della persona (ai sensi degli artt. 173, 197, 261 CPS). E' proibito caricare e/o scaricare in/da Internet file musicali, video e software che non siano attinenti alla propria mansione, come anche l'utilizzo della connessione ad Internet per motivi strettamente personali. E, inoltre, vietato l'utilizzo dei pc della scuola per la memorizzazione di materiale privato e personale.

3.2 Gestione accessi (password, backup, ecc.)

L'accesso al sistema informatico per la didattica, server e internet, nei laboratori multimediali e nelle classi sarà consentito al personale con un account dedicato, inserendo un nome utente e una password assegnati dall'Animatore Digitale o dalla Segretertia. Il personale ha la responsabilità di mantenere i suddetti dati privati e se ne vieta la divulgazione. I docenti registrano il proprio accesso scrivendo negli appositi registri la data, l'orario di utilizzo dei laboratori ed eventuali annotazione su riscontri di malfunzionamenti della strumentazione.
Le postazioni del laboratorio, così come quelle presenti nelle aule, funzionano come stazioni di lavoro e non come archivi.

3.3 E-mail

L'istituto possiede, oltre all'account di posta istituzionale, un efficiente piano di comunicazione che mette in contatto tutte le componenti della scuola interne ed esterne; esso è utilizzato unicamente per comunicazioni, in entrata e in uscita, di carattere lavorativo. Gli utenti si impegnano a non diffondere informazioni che possono nuocere alla reputazione della scuola o essere contrarie alla morale o alle leggi in vigore.

3.4 Blog e sito web della scuola

Tutti i contenuti del sito dell'Istituto sono pubblicati dall'Animatore digitale che, insieme al Dirigente scolastico, ne valuta la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy, ecc.
Il Dirigente scolastico, inoltre, si assume la responsabilità che il sito web dell'Istituto sia conforme alle linee guida di legge, in particolar modo si assicura che il lavoro pubblicato sia frutto delle attività svolte

dalla scuola e qualora fossero pubblicati lavori di altri renderà note le fonti utilizzate impegnandosi a richiedere l'autorizzazione degli stessi e a proibire la diffusione e/o la duplicazione di programmi e documenti coperti dal diritto d'autore.

3.5 Social network

Nella Scuola è in uso la piattaforma Google Workspace interamente dedicata alla didattica per creare classi virtuali, condividere risorse, realizzare contenuti multimediali, assegnare verifiche e dialogare in maniera "social" tra docenti, studenti e famiglie.

3.6 Protezione dei dati personali

Il Dirigente e il personale scolastico da questi delegato sono responsabili 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 delle proprie funzioni. Il personale incaricato deve applicare la procedura sul trattamento dei dati personali su supporto cartaceo e su supporto informatico per la protezione e la sicurezza degli stessi.
I soggetti cui si riferiscono i dati personali hanno il diritto in base all'articolo 7 del D.lgs. n. 196/2003 di verificarne l'esattezza o l'aggiornamento o l'eventuale cancellazione.

4. Strumentazione personale

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

Ai sensi del Regolamento d'Istituto non è consentito agli alunni alcun uso di strumenti elettronici personali durante le lezioni. A tale disposizione fa eccezione il caso in cui l'uso sia espressamente autorizzato dal Dirigente scolastico, su richiesta del docente di classe, per lo svolgimento di attività educative/didattiche riguardanti la scuola o in casi di estrema e comprovata urgenza per comunicazioni tra gli alunni e le famiglie.
In questi casi, ogni studente è responsabile del proprio dispositivo e non può prendere in prestito dispositivi di altri. E', inoltre, vietato usare dispositivi di registrazione audio, videocamere o fotocamere (o dispositivi che li prevedano) per registrare o fare foto in classe senza il permesso del docente e senza il permesso della persona interessata.
Non è consentito l'utilizzo di Internet per scopi diversi da quelli scolastici e giocare con i dispositivi.
L'Istituto si riserva il diritto di monitorare, controllare lle attività on-line degli alunni e di avvisare le Forze dell'Ordine quando lo ritenga necessario.
Gli studenti e le famiglie sono opportunamente informate che l'uso del cellulare è dunque vietato in classe, durante lo svolgimento delle attività didattiche; gli alunni devono spegnere il proprio telefono cellulare la mattina prima di entrare nel cancello scolastico, e riaccenderlo all'uscita solo dopo aver varcato la soglia dello stesso. Ogni infrazione sarà adeguatamente notificata attraverso provvedimenti disciplinari - richiami verbali, scritti, segnalazione al Dirigente scolastico e alle famiglie - che avranno un peso sulla valutazione dell'alunno.

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

Durante le ore di lezione, ai docenti non è consentito l'utilizzo del cellulare o dello smartphone per fini che non siano scolastici. Tali dispositivi non devono essere lasciati incustoditi e non possono essere prestati agli alunni.
E' consentito l'uso di dispositivi elettronici, ad integrazione di quelli forniti dalla scuola, e di internet

per soli fini didattici.
E' vietato usare dispositivi di registrazione audio, videocamere o fotocamere (o dispositivi che li prevedano) per registrare o fare foto in classe senza il permesso del Dirigente scolastico e senza l'autorizzazione dei genitori.
L'uso improprio verrà sanzionato in base alla normativa vigente in materia.

5.1 Prevenzione

I docenti svolgono attività di controllo degli alunni durante l'orario scolastico per evitare rischi a causa di un accesso non controllato o di un uso improprio di internet accompagnando gli alunni nella navigazione in Rete, coinvolgendoli nell'esplorazione delle opportunità e dei rischi.

Gli alunni e i genitori si impegnano a prendere visione della E–Safety Policy, a seguire le azioni promosse dalla scuola, a rispettare le regole per un uso corretto della Rete e a frequentare i corsi di formazione che la scuola organizzerà per la diffusione di informazioni legate ad un uso corretto della tecnologia digitale.

I docenti svolgeranno attività di formazione/informazione in classe adeguando le attività all'età degli alunni e avvalendosi di materiali di supporto, fra cui anche quelli messi a disposizione da "Generazioni Connesse".

La prevenzione passa poi anche attraverso percorsi di educazione all'affettività e all'emotività che già si svolgono in istituto. In collaborazione con associazioni del territorio si attueranno anche attività di sensibilizzazione alle famiglie.

- ***Rischi***

In particolare le attività si concentreranno sull'analisi dei rischi in rete maggiormente diffusi:

- ***Azioni***

Le azioni d'intervento del personale scolastico andranno ad agire su più piani:
- Informare/formare sui rischi.
- Controllo delle procedure.
- Utilizzo di firewall, filtri, software specializzati e black list.
- Collaborazione con enti esterni.

5.2 Rilevazione dei casi

La collaborazione scuola – famiglia - extra scuola è importante al fine di promuovere un utilizzo consapevole e corretto dei media e quindi oltre a condividere informazioni sulla sicurezza in rete e sui potenziali pericoli è necessario anche informare circa possibili strategie di intervento qualora si rilevassero abusi e/o infrazioni.

Cosa segnalare
1. Comportamenti inconsueti e/o inadeguati degli alunni.
2. Fatti riferiti dagli alunni e/o dalle famiglie ai docenti
3. Contenuti pericolosi inviati/ricevuti a/da altri, messi/scaricati dagli alunni

- Il docente deve segnalare **comportamenti inconsueti e/o inadeguati da parte degli alunni** nei confronti dei compagni o di altri e valutare l'accaduto.
- **I fatti accaduti** possono essere **riferiti** liberamente dagli alunni, dalle famiglie o su richiesta diretta del docente.
- Possono essere segnalati **contenuti pericolosi** inviati/ricevuti a/da altri. messi/scaricati in rete dagli alunni che comprovano l'utilizzo scorretto o criminoso degli strumenti digitali riguardanti:
  - la **privacy** (dati personali, foto e video pubblicati contro la propria volontà, ecc. …);
  - l'aggressività e la **violenza** (commenti offensivi, messaggi minacciosi, contenuti razzisti, immagini o video umilianti, informazioni false, ecc. …);
  - la **sessualità** (messaggi molesti, foto o video pornografici o pedopornografici, conversazioni private riguardanti la sessualità, ecc. …).

- **Come segnalare**

Il docente che riceve la segnalazione deve provvedere a informare il Referente del bullismo/cyberbullismo e/o componenti della commissione e/o il collaboratore del dirigente che provvederanno ad inserire la segnalazione nel registro apposito.

Strumenti da utilizzare
4. Annotazione del comportamento sul registro elettronico e comunicazione scritta sul diario ai genitori.
5. Convocazione scritta e colloquio con i genitori degli alunni, da parte dei docenti
6. Diario di bordo (allegato)
7. Relazione scritta al Dirigente scolastico

La legge rimette ai genitori dell'alunno la scelta di richiedere l'ammonizione del colpevole attraverso la querela, per quanto riguarda i reati meno gravi.
Per i reati più gravi, i docenti hanno l'obbligo di allertare le autorità competenti e di presentare la denuncia qualora se ne avvisino gli estremi di reato.
Nella denuncia dovrà essere esplicitato:

- ✔ il fatto e il giorno dell'acquisizione del fatto;
- ✔ le fonti di prova;
- ✔ le generalità e il domicilio della persona a cui è attribuito il reato;
- ✔ la persona offesa;
- ✔ i testimoni.

Il Dirigente scolastico, l'equipe pedagogica e/o il Consiglio di classe ha la possibilità di sostituire le sanzioni disciplinari più severe con altri provvedimenti, comprendenti altre attività a scopo sociale (ricerche e/o attività di studio ed approfondimento coerenti con l'infrazione commessa) che possono utilmente costituire un rimedio ed un monito.

A chi rivolgersi per chiedere aiuto
1. Ai genitori
2. Al dirigente scolastico

3. Al referente del Bullismo e del Cyberbullismo
4. Ai docenti
5. Alla polizia postale
6. Alla Chat di Telefono Azzurro
7. Alla helpline di Generazione Connesse, al numero gratuito 1.96.96.
8. A Save the Children

5.3 Gestione dei casi

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

1. Gestione dei casi di "immaturità"
2. I comportamenti cosiddetti "quasi aggressivi"
3. la presa in giro "per gioco".

Sono controllati e contenuti dai docenti attraverso i normali interventi educativi, di richiamo al rispetto delle regole di convivenza civile e democratica, di rispetto degli altri, per evitare che possano degenerare, diventare pericolosi per sé o offensivi e minacciosi per gli altri.

4. Gestione dei casi di "prepotenza" o "prevaricazione".
5. I comportamenti definibili "Bullismo" (per la costanza e ripetitività nel tempo, l'asimmetria delle forze in gioco, il disagio della vittima).

I comportamenti definibili "Bullismo" possono esprimersi nelle forme più varie e non sono tratteggiabili a priori, se non contestualizzandoli.

6. Nel caso particolare del "Cyberbullismo" le molestie sono attuate attraverso strumenti tecnologici.

Per prevenire e affrontare il bullismo dunque i docenti non solo identificano vittime e prepotenti in divenire, ma tutti insieme affrontano e intervengono sul gruppo-classe, coinvolgendo i genitori degli allievi. L'elemento fondamentale per una buona riuscita dell'intervento educativo è infatti la corretta, compiuta e convinta ristrutturazione dell'ambiente sociale in cui tale fenomeno si verifica, e in particolare delle relazioni nel contesto della classe. Gli atteggiamenti degli alunni, così come quelli dei loro genitori, possono giocare un ruolo molto significativo nel ridurre la dimensione del fenomeno. Gli interventi mirati sul gruppo classe sono gestiti in collaborazione dal team dei docenti della classe e d'intesa con le famiglie - ad esempio con percorsi di mediazione volta alla gestione positiva del conflitto, con gruppi di discussione (circle time), con rappresentazioni e attività di role-play sull'argomento del bullismo, con le strategie del problem solving. Vengono intrapresi anche i percorsi individualizzati di sostegno alle vittime, volti a incrementarne l'autostima e l'assertività e a potenziare le risorse di interazione sociale, mentre i prevaricatori sono destinatari di interventi mirati a smuoverne le competenze empatiche e a favorire una loro condivisione delle norme morali.
Inoltre la scuola, qualora rilevi una situazione psico-socio-educativa particolarmente problematica, convoca i genitori o gli esercenti la potestà per valutare con loro a quali risorse territoriali possono rivolgersi. Consiglia altresì di servirsi dello sportello di ascolto psicologico gratuito se attivo presso la scuola.

7. Gestione degli "abusi sessuali".

Lo spettro delle forme di abuso e di violenza è diventato ancora più ampio e subdolo in seguito alle possibilità offerte dai nuovi mezzi di comunicazione come internet, il cellulare o altri dispositivi tecnologici, e il loro utilizzo sempre più diffuso non fa che acuire il problema. Internet, infatti, permette di scaricare o vendere immagini o filmati di pornografia infantile.
La denuncia all'autorità giudiziaria o agli organi di Polizia, da parte degli insegnanti o del Dirigente scolastico, costituisce il passo necessario per avviare un intervento di tutela a favore della vittima e attivare un procedimento penale nei confronti del presunto colpevole. Il compito della scuola non è

comunque solo quello di "segnalare", ma più ampio ed importante, soprattutto nella prevenzione dell'abuso, nonché nella ripresa della piccola vittima, in quanto ha al suo interno fattori relazionali ed educativi che possono aiutare il bambino a riprendere una crescita serena. A tal fine la scuola lavora insieme alle altre figure professionali e alle famiglie, scambiando informazioni e condividendo progetti e prassi operative, favorendo le occasioni di confronto e di dialogo.

Annessi

1. Procedure operative per la gestione delle infrazioni alla Policy. (allegato 1)

✔ ascoltare e capire le problematiche dell'alunno, emerse dall'utilizzo della Rete.
✔ coinvolgere i genitori, rispettando i diritti dell'alunno.
✔ informare il Referente per il bullismo e cyberbullismo, il referente dell'E–Safety e gli operatori scolastici.
✔ in caso di gravi abusi, informare le autorità competenti.
✔ rimuovere i contenuti pericolosi online.
✔ invitare i compagni a supportare l'alunno in difficoltà.
✔ deresponsabilizzare la vittima.
✔ proporre discussioni di gruppo e coinvolgere la comunità scolastica in percorsi di prevenzione.

2. Procedure operative per la protezione dei dati personali. (allegato 2)

In ottemperanza al codice sulla privacy (Decreto Legislativo n. 196/2003, codice in materia di protezione dei dati personali) tutti i dati personali dei componenti della comunità scolastica devono:
✔ essere trattati in modo lecito.
✔ Essere raccolti e registrati per scopi specifici, espliciti e legittimi.
✔ Essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati

3. Procedure operative per la rilevazione, il monitoraggio e la gestione delle segnalazioni. (allegato3)

Per la rilevazione, il monitoraggio e la gestione delle segnalazione saranno attuate le seguenti procedure:
✔ Compilazione di un "Diario di bordo" della scuola nel quale riportare le situazioni problematiche online segnalate. (modello proposto da "Generazioni connesse").

4. Procedure operative per la gestione dei casi.

Procedura operativa in caso di pericolo online:

✔ ascoltare e capire le problematiche dell'alunno, emerse dall'utilizzo della Rete.
✔ coinvolgere i genitori, rispettando i diritti dell'alunno.
✔ informare il Referente per il bullismo e cyberbullismo, il referente dell'E–Safety e gli operatori scolastici.

✔ in caso di gravi abusi, informare le autorità competenti.
✔ rimuovere i contenuti pericolosi online.
✔ invitare i compagni a supportare l'alunno in difficoltà.
✔ deresponsabilizzare la vittima.
✔ proporre discussioni di gruppo e coinvolgere la comunità scolastica in percorsi di prevenzione.
✔ compilare il "Diario di bordo" per poter tenere traccia di ciò che è avvenuto rispetto ai comportamenti degli alunni online e di come è stato gestito il problema.

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

L'Istituto non ha siglato protocolli con le forze dell'ordine o con i servizi messi a disposizione nel territorio per la gestione condivisa dei casi, ma ha concordato e organizzato ricorrenti forme di collaborazione nella prevenzione e contrasto del bullismo e del cyberbullismo con la Polizia dello Stato e con associazioni del settore.

ALLEGATO N°1
Procedure operative per la gestione delle infrazioni alla Policy.

EPISODIO SEGNALATO	ISTIGATORE		VITTIMA	
	frequenza	Provvedimento	Organo	Intervento
Bullismo e Cyberbullismo				
Comportamenti verbali deliberatamente ostili e provocatori nei confronti di compagni, insegnanti e personale non docente: l'invio di messaggi elettronici, violenti e volgari allo scopo di suscitare conflitti verbali.	1° volta 2° volta	Richiamo verbale e colloquio con la famiglia Ammonizione scritta sul registro e convocazione della famiglia	Docente	I docenti: colloquio individuale con la vittima ed eventuale orientamento allo sportello di ascolto; sensibilizzazione e coinvolgimento del gruppo classe per supportare le difficoltà;

	Ulteriori episodi	Come da Regolamento di Istituto	Consiglio di classe	informazione e coinvolgimento della famiglia. Il Dirigente Scolastico: In caso di reiterazione di atti nei confronti della stessa vittima, deciderà se il fatto vada riportato alle autorità di competenza.
Sexting Invio e condivisione di testi o immagini sessualmente esplicite tramite internet o telefono cellulare	In caso di segnalazione, gli episodi di sexting o grooming verranno valutati singolarmente e - previo coinvolgimento della famiglia - si stabilirà la modalità d'intervento e l'eventuale comunicazione agli organi competenti.			
Grooming Adescamento di un minore in internet tramite manipolazione psicologica volta a superarne le resistenze, a ottenerne la fiducia e abusarne sessualmente				

EPISODIO SEGNALATO	ISTIGATORE		VITTIMA	
	frequenza	Provvedimento	Organo	Intervento
Fatti gravi o parole che consapevolmente tendono ad emarginare gli altri studenti:				

Harassment Molestie persistenti e ripetute, dirette verso una persona specifica, che possono causare disagio emotivo e psichico. **Cyberstalking** Comportamenti che, attraverso l'uso delle nuove tecnologie, sono finalizzati a perseguitare le vittime in diversi modi e hanno lo scopo di infastidirle e molestarle, sino a commettere atti di aggressione molto più violenti, anche di tipo fisico. **Denigration** Distribuzione, all'interno della rete o tramite SMS, di messaggi falsi o dispregiativi nei confronti delle vittime, con lo scopo "di danneggiare la reputazione o le amicizie di colui che viene preso di mira". **Exclusion** Esclusione intenzionale di un pari dal proprio gruppo di amici, dalla chat o da un gioco interattivo.	1° volta 2° volta	Richiamo verbale Ammonizione scritta Ammonizione scritta sul diario e sul registro	Docente	I docenti: colloquio individuale con la vittima, con la famiglia ed eventuale orientamento allo sportello di ascolto; sensibilizzazione e coinvolgimento del gruppo classe per supportare le difficoltà;
	Ulteriori episodi	Sospensione dalle visite guidate, viaggi d'istruzione, gruppi sportivi ed altre attività con obbligo della presenza a scuola Abbassamento del voto condotta Diffida scritta con comunicazione alla famiglia da parte del Dirigente Scolastico	Consiglio di classe Dirigente scolastico	informazione e coinvolgimento della famiglia. Il Dirigente Scolastico: In caso di reiterazione di atti nei confronti della stessa vittima, deciderà se il fatto vada riportato alle autorità di competenza.

Allegato N°3

PROGETTO GENERAZIONI CONNESSE

MODULO PER LA SEGNALAZIONE DI CASI

Nome di chi compila la segnalazione: Ruolo:

Data: Scuola:

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

MODULO PER IL FOLLOW-UP DEI CASI

	AZIONI INTRAPRESE	La situazione è
Aggiornamento 1		□ migliorata □ invariata □ peggiorata Come:
Aggiornamento 2		□ migliorata □ invariata □ peggiorata Come:
Aggiornamento 3		□ migliorata □ invariata □ peggiorata Come:
Aggiornamento 4		□ migliorata □ invariata □ peggiorata Come:
Aggiornamento 5		□ migliorata □ invariata □ peggiorata Come:
Aggiornamento 6		□ migliorata □ invariata □ peggiorata Come:
Aggiornamento 7		□ migliorata □ invariata □ peggiorata Come:
Aggiornamento 8		□ migliorata □ invariata □ peggiorata Come:

LA "NETIQUETTE"

Fra gli utenti dei servizi telematici di rete si è sviluppata nel corso del tempo, una serie di tradizioni e di norme di buon uso che costituiscono il ***Galateo della rete***. La persona che fa uso di TIC deve rispettare le seguenti regole:

a. **Non essere offensivo.** Il testo è l'unico mezzo attraverso il quale comunicare con gli altri in rete. Il tono della voce, l'espressione del viso, non possono essere di aiuto per far comprendere all'altro il senso del discorso. Il rischio di essere fraintesi è altissimo. Bisogna tenerlo sempre presente quando si scrive ed usare gli emoticons (emotional icons) per ribadire il tono del messaggio: ;-) scherzoso; ☺ allegro; :o (triste e così via).

b. **Seguire regole di comportamento analoghe alle proprie regole di vita.** Esprimere le proprie idee, nei limiti dell'educazione e del rispetto altrui. Utilizzare in maniera fraudolenta un prodotto a pagamento equivale ad un furto. Solo acquistandolo regolarmente s'incoraggiano i realizzatori a creare altri prodotti.

c. **Scegliere l'ambiente adatto a se stessi.** Ogni chat, mailing list, newsgroup, forum ha delle caratteristiche specifiche e non si può trovare sempre argomenti adatti a noi o di nostro interesse. Scegliere la community che si avvicina di più alle proprie esigenze, ma soprattutto quella dove ci si sente più a nostro agio, anche grazie al controllo del moderatore.

d. **Scegliere di essere paziente e comprensivo.** Quando s'invia un messaggio non bisogna pretendere risposta. Chi comunica con noi può non essere interessato all'argomento che proponiamo oppure può non avere il tempo di rispondere.

e. **Scegliere toni moderati.** Se si esprime il parere in maniera pacata è meno probabile che le parole usate possano provocare reazioni dure da chi comunica con noi. Basta poco per infiammare una discussione e serve invece molto tempo per tornare ad un dialogo tranquillo.

f. **Rispettare la privacy.** Usare in rete la stessa regola che usi nella vita. Ognuno di noi ha il diritto di scegliere se condividere o meno le informazioni che lo riguardano.

g. **Non abusare delle proprie conoscenze.** Non usare mai le proprie competenze per entrare nel mondo altrui. Non rendere pubbliche le conversazioni private. Non inviare fotografie proprie o di altre persone.

h. **Trascurare gli errori degli altri.** Il desiderio di rispondere velocemente porta ad errori di digitazione, di grammatica o di sintassi ma l'importante è che il messaggio sia compreso. Non siate intolleranti con chi ha scarsa dimestichezza con le TIC o commette errori concettuali.

i. **Dimenticare le differenze.** La rete è un mondo nel quale l'unico strumento è la tastiera, l'unico oggetto visibile il monitor. Rispettate le persone diverse per nazionalità, cultura, religione, sesso: il razzismo e ogni tipo di discriminazione sociale non sono ammessi.

j. **Presentarsi con cura.** In rete si hanno solo le parole per farsi conoscere. Bisogna usarle con cura, scegliendo quelle di cui si è veramente convinti, solo così daremo a chi comunica con noi l'impressione di come siamo veramente.

k. **Utilizzare la rete per ampliare le tue conoscenze.** Internet è una sterminata enciclopedia a portata di mouse ed offre anche la possibilità di leggere le opinioni degli altri su qualsiasi argomento. Si possono trovare informazioni specialistiche, il materiale per una ricerca scolastica ma anche solo confrontare la propria opinione.

l. **Essere prudente.** Non rivelare dettagli o informazioni personali o di altre persone (indirizzi, numeri di telefono). Non accettare senza riflettere di incontrare qualcuno che si è appena conosciuto nella rete. Non credere a tutto quello che viene detto perché non si può avere la certezza dell'identità della persona con la quale si sta comunicando).

m. **Non urlare.** Scrivere in maiuscolo su Internet equivale ad urlare: è uno strumento a disposizione per enfatizzare le cose che stai dicendo. Attenzione a non abusarne. Se si incontrano in internet immagini o scritti che infastidiscono o se qualcuno non rispetta queste regole è opportuno parlane con gli insegnanti o con i genitori.

Roma, 24 novembre 2023