ISTITUTO COMPRENSIVO DI Fenegrò

ANNO SCOLASTICO 2019/2020

E-SAFETY POLICY

Delibera del Collegio dei Docenti n.
Delibera del Consiglio d'Istituto n.

INDICE

5.2 - Rilevazione

a) Che cosa segnalare
b) Come segnalare e a chi.
c) Come gestire le segnalazioni.
d) Procedure operative per la rilevazione, il monitoraggio e la gestione delle segnalazioni

5.3- Gestione dei casi

a) *Definizione delle azioni da intraprendere a seconda della specifica del caso*
b) *Procedure operative per la gestione dei casi.*

ALLEGATI:

1) cosa fare cyberbullismo
2) cosa fare sexting
3) cosa fare adescamento
4) diario bordo scuola
5) vademecum
6) Kit didattico GenerazioniConnesse-Kids
7) Kit didattico GenerazioniConnesse-Teens
8) Kit didattico GenerazioniConnesse-Docenti

1. INTRODUZIONE

1.1 Premessa

Una delle finalità educative del nostro Istituto è quella di favorire la formazione armonica della personalità degli alunni per rendere possibile un'adeguata integrazione sociale. Tale integrazione, nella società attuale, avviene in larga misura anche attraverso strumenti digitali che permettono la connessione ad internet e ai social network. I nostri bambini/ragazzi sono dunque "nativi digitali : essi socializzano, interagiscono, comunicano, giocano, studiano attraverso tecnologie multimediali che, se usate in modo non responsabile, li espongono a rischi di cui loro stessi, a volte, non sono nemmeno consapevoli.
Con una diffusione apparentemente sconfinata delle tecnologie dell'informazione nella vita quotidiana, è necessario che la scuola, in quanto ente formativo, non promuova solo l'alfabetizzazione digitale, ma educhi i propri alunni ad una cittadinanza digitale consapevole e responsabile.

1.2 Scopo della Policy

La Policy di e-safety è un documento, autoprodotto dalla scuola, attraverso il quale si esplicitano i parametri di sicurezza digitale, le norme comportamentali e le procedure per l'utilizzo delle TIC in ambiente scolastico, nonché le misure per la prevenzione, per la rilevazione e la gestione delle problematiche connesse ad un uso non corretto di tali tecnologie.

1.3 Ruoli e Responsabilità

Tutta la Comunità Scolastica è tenuta al rispetto delle norme e dei protocolli contenuti nel presente documento e si impegna ad un uso responsabile delle TIC, al fine di salvaguardare la sicurezza e i diritti di tutti i Cittadini digitali (ovvero tutti coloro che si connettono ad Internet attraverso dispositivi multimediali, in ambiente scolastico ed extrascolastico)**.**
Il personale scolastico è tenuto a vigilare, nei limiti delle proprie competenze e possibilità, affinché il presente regolamento sia rispettato e a segnalare le infrazioni secondo le procedure illustrate nel presente documento.
Studenti e genitori possono segnalare al personale scolastico eventuali infrazioni di cui siano venuti a conoscenza o situazioni di disagio che li vedano direttamente coinvolti in qualità di vittime. In particolare:

DS:

- provvede periodicamente alla revisione, in collaborazione con il team per l'innovazione digitale, il Collegio dei docenti ed il Consiglio d'Istituto, della e-policy ed alla sua integrazione con il regolamento d'istituto;

TID:

- provvede periodicamente all' aggiornamento della e-policy anche in funzione dell'evoluzione delle tecnologie digitali;

DOCENTI:

- promuovono la cultura dell'uso consapevole e corretto delle nuove tecnologie e della rete, del rispetto della dignità e della privacy di ciascuno;
- prevengono e intercettano situazioni legate ad un uso scorretto delle nuove tecnologie e ai rischi della rete;
- vigilano, nei limiti delle proprie competenze e possibilità, sull'uso scolastico delle nuove tecnologie e della rete;
- applicano la e-policy;
- suggeriscono al TID modifiche ed integrazioni alla stessa;
- si impegnano al pieno rispetto della e-policy;

GENITORI: si impegnano a:

- collaborare con la scuola nella promozione della cultura dell'uso consapevole e corretto delle nuove tecnologie e della rete, del rispetto della dignità e della privacy di ciascuno;
- prevengono e intercettano situazioni legate ad un uso scorretto delle nuove tecnologie e le segnalano alla scuola;
- vigilano, nei limiti delle proprie competenze e possibilità, sui device dei propri figli al fine di prevenire ed intercettare situazioni di rischio;
- segnalano alla scuola casi di uso scorretto delle nuove tecnologie da parte di alunni singoli o in gruppo;
- suggeriscono alla scuola modifiche ed integrazioni alla e-policy;

ALUNNI: si impegnano a:

- rispettare la e-policy;
- segnalare tempestivamente casi di uso scorretto delle nuove tecnologie da parte di compagni singoli o in gruppo;
- collaborare con la scuola nella diffusione dell'uso corretto delle tecnologie digitali;
- suggerire alla scuola modifiche ed integrazioni alla e-policy;

DSGA:

- suggerisce al TID modifiche ed integrazioni alla stessa;

PERSONALE ATA: si impegna a:

- collaborare con il DS, il DSGA e i docenti nella prevenzione ed intercettazione di situazioni legate ad un uso scorretto delle nuove tecnologie;
- al pieno rispetto della e-policy;

ORGANO DI GARANZIA INTERNO:

- in caso di sanzioni disciplinari, garantisce la corretta applicazione della e-policy e del regolamento d'istituto, nella salvaguardia dei diritti degli alunni;

1.4 Condivisione e comunicazione della Policy all'intera comunità scolastica

Il presente documento, prodotto e revisionato dal TID, è condiviso con il Collegio dei Docenti e con il Consiglio d'Istituto che possono apportare eventuali modifiche ed integrazioni. Dopo

l’approvazione degli Organi Collegiali preposti, il documento deve essere pubblicato sul sito scolastico affinché l’intera Comunità Scolastica possa visionarlo.

1.5 Gestione delle infrazioni alla Policy

Le infrazioni al regolamento potranno portare all'irrogazione di sanzioni disciplinari.
Vedasi regolamento disciplina alunni

1.6 Monitoraggio dell'implementazione della Policy e suo aggiornamento

Il TID, sulla base delle segnalazioni effettuate, rileva annualmente le esigenze dell'Istituto verificando che il documento sia una risorsa efficace, operando eventuali integrazioni o modifiche.

1.7 Integrazione della Policy con Regolamenti esistenti

Il TID e la referente per il bullismo, in collaborazione con la Commissione POF, in raccordo con il Collegio Docenti, opera al fine di integrare i regolamenti dell'Istituto con il presente documento, apportandone le opportune modifiche da proporre al Consiglio d'Istituto.

2. FORMAZIONE E CURRICOLO

2.1 Curricolo sulle competenze digitali per gli studenti

COMPETENZA DIGITALE	
Dalle Raccomandazione del Parlamento Europeo e del Consiglio del 18 dicembre 2006 - 2006/962/CE . ***La competenza digitale*** *consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione per il lavoro, il tempo libero e la comunicazione. Essa implica abilità di base nelle tecnologie dell'informazione e della comunicazione (TIC): l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet.*	
Dalle Indicazioni Nazionali per il curricolo della scuola dell'infanzia e del primo ciclo d'istruzione (2012) ***Profilo della competenza al termine del primo ciclo di istruzione.*** *Ha buone competenze digitali, usa con consapevolezza le tecnologie della comunicazione per ricercare e analizzare dati ed informazioni, per distinguere informazioni attendibili da quelle che necessitano di approfondimento, di controllo e di verifica e per interagire con soggetti diversi nel mondo.*	
SCUOLA PRIMARIA	**SCUOLA SECONDARIA**
Dall'all. A modello di certificazione sc. Primaria – DM 742/2017 *Usa con responsabilità le tecnologie in contesti comunicativi concreti per ricercare informazioni e per interagire con altre persone, come supporto alla creatività e alla soluzione di problemi semplici.*	**Dall'all. B modello di certificazione sc. Secondaria – DM 742/2017** *Utilizza con consapevolezza e responsabilità le tecnologie per ricercare, produrre ed elaborare dati e informazioni, per interagire con altre persone, come supporto alla creatività e alla soluzione di problemi.*

SCUOLA DELL'INFANZIA
TRASVERSALE A TUTTI I CAMPI D'ESPERIENZA

CURRICOLO VERTICALE DI COMPETENZE DIGITALI				
Informazione	comunicazione	creazione	sicurezza	problem solving
DISCIPLINE CONCORRENTI: TUTTE				

SCUOLA PRIMARIA
TRAGUARDI PER LO SVILUPPO DELLE COMPETENZE AL TERMINE DELLA SCUOLA PRIMARIA
Utilizzare con dimestichezza le più comuni tecnologie dell'informazione e della comunicazione, in contesti comunicativi concreti per ricercare dati e informazioni e per interagire con soggetti diversi. Essere consapevole delle potenzialità, dei limiti e dei rischi dell'uso delle tecnologie dell'informazione e della comunicazione.
CONOSCENZE
FINE QUINTA
Semplici applicazioni tecnologiche quotidiane e relative modalità di funzionamento I principali dispositivi informatici di input e output I principali software applicativi utili per lo studio, con particolare riferimento alla videoscrittura, alle presentazioni e ai giochi didattici Semplici procedure di utilizzo di Internet per ottenere dati, fare ricerche, comunicare Rischi fisici nell'utilizzo di apparecchi elettrici ed elettronici Rischi nell'utilizzo della rete con PC e telefonini .

INFORMAZIONE	
FINE QUINTA	
ABILITÀ (desunte dal curricolo di competenze digitali)	- Avviare alla conoscenza della Rete per scopi di informazione, - Accedere all'informazione online, effettuare ricerche online - Utilizzare semplici materiali digitali per l'apprendimento. - Manipolare e salvare informazioni e contenuto in modo da rendere più facile il recupero - Organizzare informazioni e dati.

COMUNICAZIONE	
FINE QUINTA	
ABILITÀ	

(desunte dal curricolo di competenze digitali)	- Utilizzare consapevolmente le più comuni tecnologie, conoscendone i principi di base, soprattutto in riferimento alle apparecchiature digitali domestiche. - Utilizzare il PC, alcune periferiche e programmi applicativi. - Avviare alla conoscenza della Rete per scopi di comunicazione - Usare le tecnologie e i media per lavori in gruppo

CREAZIONE	
FINE QUINTA	
ABILITÀ (desunte dal curricolo di competenze digitali)	- Creare contenuti in diversi formati inclusi i multimedia. - Editare e perfezionare contenuti prodotti in prima persona o da altri. - Esprimersi in modo creativo attraverso i media digitali e le tecnologie. - Modificare, selezionare ed integrare risorse esistenti per creare conoscenza e contenuti nuovi.

SICUREZZA	
FINE QUINTA	
ABILITÀ (desunte dal curricolo di competenze digitali)	- Proteggere i propri strumenti ed essere consapevole dei rischi in rete e delle minacce; conoscere le misure di protezione e sicurezza. - 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.

PROBLEM SOLVING	
FINE QUINTA	
ABILITÀ (desunte dal curricolo di competenze digitali)	- Identificare possibili problemi e risolverli (dalla risoluzione di problemi semplici a problemi più complessi) con l'aiuto di strumenti digitali. - Partecipare attivamente in produzioni collaborative digitali e multimediali. - Esprimere se stessi in modo creativo attraverso i media digitali e le tecnologie;

SCUOLA SECONDARIA

TRAGUARDI PER LO SVILUPPO DELLE COMPETENZE AL TERMINE DELLA SCUOLA SECONDARIA

Utilizzare con dimestichezza le più comuni tecnologie dell'informazione e della comunicazione, individuando le soluzioni potenzialmente utili ad un dato contesto applicativo, a partire dall'attività di studio, per ricercare e analizzare dati ed informazioni in modo pertinente e per distinguere informazioni attendibili.
Essere consapevole delle potenzialità, dei limiti e dei rischi dell'uso delle tecnologie dell'informazione e della comunicazione, con particolare riferimento al contesto culturale e sociale in cui vengono applicate.

CONOSCENZE

FINE TERZA

Le applicazioni tecnologiche quotidiane e le relative modalità di funzionamento. I dispositivi informatici di input e output. Il sistema operativo e i più comuni software applicativi. 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. 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.

.

INFORMAZIONE	
FINE TERZA	
ABILITÀ (desunte dal curricolo di competenze digitali)	- Navigare, ricercare e filtrare le informazioni - Effettuare ricerche online. - Raccogliere, comprendere e valutare in modo critico le informazioni. - Manipolare e salvare informazioni e contenuto in modo da rendere più facile il recupero. - Organizzare informazioni e dati.

COMUNICAZIONE	
FINE TERZA	
ABILITÀ	

(desunte dal curricolo di competenze digitali)	- Interagire attraverso l'impiego di dispositivi digitali ed applicazioni. - Somprendere come si articola, si realizza e gestisce la comunicazione digitale; - Selezionare opportune modalità di comunicazione con l'impiego di strumenti digitali; - Adattare le modalità e la strategia di comunicazione a specifici destinatari. - Condividere con altri localizzazione e contenuto delle informazioni reperite. - Essere disponibile ed in grado di condividere conoscenze, contenuti e risorse; agire come mediatori. - Sapercorrettamente citare le fonti ed integrare nuove informazioni all'interno di conoscenze già possedute. - Usare le tecnologie e i media per lavori in gruppo. - Conoscere e sapere applicare norme di comportamento per l'interazione in rete/ virtuale; - Essere in grado di proteggere se stessi e gli altri da possibili pericoli in rete (per esempio il cyberbullismo) - Sviluppare strategie attive per individuare comportamenti inappropriati. - Essere in grado di proteggere la reputazione in rete.

CREAZIONE	
FINE TERZA	
ABILITÀ (desunte dal curricolo di competenze digitali	- Creare contenuti in diversi formati inclusi i multimedia. - Editare e perfezionare contenuti prodotti in prima persona o da altri. - Esprimersi in modo creativo attraverso i media digitali e le tecnologie. - Modificare, selezionare ed integrare risorse esistenti per creare conoscenza e contenuti nuovi. - Comprendere come si applicano le norme relative al diritto d'autore e licenze alle informazioni e contenuti.

SICUREZZA	
FINE TERZA	
ABILITÀ (desunte dal curricolo di competenze digitali	- Proteggere i propri strumenti ed essere consapevole dei rischi in rete e delle minacce. - Proteggere i dati personali. - Rispettare la privacy di altri soggetti. - Proteggersi dalle frodi in rete, dalle minacce e dal cyberbullismo. - Evitare i rischi per la salute connessi all'uso della tecnologia relativamente a minacce al benessere fisico e psicologico. - Essere consapevole dell'impatto delle tecnologie dell'informazione e comunicazione sull'ambiente.

PROBLEM SOLVING	
FINE TERZA	
ABILITÀ (desunte dal curricolo di competenze digitali	- Identificare possibili problemi(dai più semplici ai più complessi) e risolverli con l'aiuto di strumenti digitali - Partecipare attivamente in produzioni collaborative digitali e multimediali. - Esprimere se stessi in modo creativo attraverso i media digitali e le tecnologie. - Produrre conoscenza e risolvere problemi concettuali con il supporto di strumenti digitali. - Comprendere dove le proprie competenze possono essere migliorate o accresciute

In allegato, è disponibile il kit didattico predisposto da Generazioni Connesse, composto da tre e-book interattivi per bambini, ragazzi e insegnanti, con consigli e giochi per navigare sicuri online. In particolare, l'e-book dedicato ai docenti approfondisce alcune tematiche legate all'utilizzo di Internet e nuovi media offrendo spunti di riflessione e attività didattiche per condurre laboratori con bambini e ragazzi

2.2 Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica

Per poter promuovere l'utilizzo e l'integrazione delle TIC nella didattica e per formare gli alunni ad un uso consapevole e sicuro di internet l'Istituto prevede la partecipazione al percorso di formazione promosso dal MIUR nell'ambito del PNSD organizzato dagli snodi formativi rivolta ad Animatore Digitale, Team per l'innovazione e ai docenti della scuola

2.3 Sensibilizzazione delle famiglie

La scuola invita i genitori ad assumersi l'incarico di accompagnare i figli verso le molteplici possibilità della rete, aiutandoli a riconoscerne ed evitarne i rischi.
Durante le prime riunioni di classe i docenti suggeriscono la consultazione del portale Generazioni Connesse, dotato di una specifica Area Genitori, dove è possibile reperire informazioni e consigli pratici per un'equilibrata e consapevole gestione del rapporto tra bambini, ragazzi e media.
La scuola è impegnata anche a partecipare agli eventi che il MIUR organizza annualmente con giornate dedicate alla sicurezza in internet e alla lotta contro il bullismo e cyber-bullismo, pianificando percorsi didattici da realizzare nelle classi.

3. GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE SCOLASTICA

3.1 Protezione delle strumentazioni e della navigazione

La scuola dovrà dotarsi entro il triennio di tutte le strumentazioni tecniche necessarie per :

- Proteggere la privacy del personale scolastico, degli alunni e delle loro famiglie, soprattutto per quel che riguarda i dati sensibili.
- Garantire la navigazione sicura nei computer dell'Istituto.

Rivolgendosi a personale tecnico qualificato, la scuola dovrà dotarsi di:

- Antivirus (software per il monitoraggio e la rimozione di virus, spyware, adware).
- Browser protetti (controllo parentale e classificazione di contenuti, eventualmente anche browser specifici per bambini).
- Filtri (sistemi in grado di bloccare in modo automatico l'utilizzo di determinati servizi o l'accesso a siti e contenuti potenzialmente dannosi per bambini e adolescenti. Alcuni software bloccano le informazioni in entrata, come le e-mail o impediscono che i bambini forniscano informazioni riservate come il proprio nome, l'indirizzo o il numero di telefono).
- Utenti diversificati (Utente docente protetto da password e utente alunni con restrizioni).

3.2 Gestione accessi

a) Accesso alle strumentazioni scolastiche

Il personale scolastico è tenuto a seguire le seguenti regole di accesso alle strumentazioni:

- È consentito l'uso delle strumentazioni scolastiche esclusivamente per uso didattico. Usi diversi da questo vanno autorizzati dal Dirigente Scolastico.
- Le strumentazioni scolastiche devono essere maneggiate con attenzione al fine di evitarne danni strutturali.
- Le strumentazioni, dopo essere state utilizzate, vanno riposte con cura e non separate dagli accessori d'uso (caricabatterie, mouse…).
- Il personale scolastico è tenuto a segnalare tempestivamente al responsabile della custodia delle strumentazioni la mancanza delle stesse o di eventuali accessori.
- Le strumentazioni vanno custodite in appositi armadi provvisti di serratura. Laddove ciò non fosse possibile, il personale ATA provvederà a chiudere a chiave la classe al termine delle lezioni.
- Il personale docente non è tenuto a creare nuovi utenti sulle strumentazioni scolastiche.
- L'utente riservato ai docenti deve essere provvisto di password (che non deve essere comunicata in nessun casi agli alunni)
- Non è consentito il salvataggio di documenti personali (bollette telefoniche, cedolini stipendi, ecc).
- È vietato installare software di uso non didattico

Gli alunni sono tenuti a rispettare le seguenti regole d'accesso alle strumentazioni:

- È consentito l'uso delle strumentazioni scolastiche esclusivamente per uso didattico, secondo le disposizioni del docente presente.
- Le strumentazioni, dopo essere state utilizzate, vanno riposte con cura e non separate dagli accessori d'uso (caricabatterie, mouse…)
- Le strumentazioni scolastiche devono essere maneggiate con attenzione al fine di evitarne danni strutturali.
- Gli alunni possono accedere solo all'utente a loro riservato, libero da password.
- È consentito il salvataggio di documenti personali a scopo didattico, utilizzando cartelle specifiche per ciascuna classe.

-

b) Accesso alla rete

In ogni plesso è presente un modem-router che permette la messa in rete e la connessione ad internet dei dispositivi presenti nell'edificio. Per accedere alla rete è necessario che il dispositivo sia collegato tramite cavo o con Wi-Fi.
Per connettere un dispositivo al Wi-Fi scolastico è necessario inserire la chiave di sicurezza, custodita dall'Amministratore delle reti. Le responsabili di plesso possono richiedere tale codice per connettere dispositivi di operatori esterni, avendo cura di tenerlo riservato.
Nella scuola secondaria, devono essere presenti due reti separate: una riservata alla segreteria e una didattica. Le due reti non devono comunicare tra loro al fine di garantire la riservatezza dei dati di segreteria.

c) Accesso ad internet

Il personale scolastico è tenuto a seguire le seguenti regole di accesso ad Internet:

- È possibile accedere ad internet attraverso strumentazioni in dotazione all'istituto o attraverso dispositivi personali
- L'accesso ad internet e la navigazione attraverso le strumentazioni scolastiche è riservato ad un uso strettamente didattico
- È possibile accedere ad account personali durante l'uso di internet, ma è obbligatorio il logout al termine
- Non è consentito il salvataggio di dati personali (nomi utenti, account e password) nei browser delle strumentazioni scolastiche
- È vietato scaricare o installare da internet materiale potenzialmente dannoso, di provenienza non sicura o non legale

Gli alunni sono tenuti a rispettare le seguenti regole d'accesso ad internet:

- È vietato l'accesso ad internet senza autorizzazione da parte del personale docente
- È vietata la navigazione in assenza del docente
- L'accesso ad internet e la navigazione attraverso le strumentazioni scolastiche è riservato ad un uso strettamente didattico e nel rispetto di diritti della cittadinanza digitale e delle norme vigenti di utilizzo legale della rete.
- È vietato il salvataggio di dati personali (nomi utenti, account e password) nei browser delle strumentazioni scolastiche.
- È vietato scaricare da internet materiale senza l'autorizzazione del docente

Tutti gli operatori presenti a qualsiasi titolo nella scuola (esperti esterni, collaboratori, ditte esterne...) e i genitori che accedono all'edificio scolastico, dovranno attenersi alle regole generali previste per il personale.

3.3 E-mail

Tutte le comunicazioni scolastiche dovranno progressivamente avvenire attraverso canali digitali.
Il personale scolastico, le famiglie, gli operatori esterni e gli Enti potranno comunicare con la segreteria inviando la posta ai due indirizzi a disposizione dell'Istituto:
coic82200c@istruzione.it; coic82200c@pec.istruzione.it

La gestione di questi due indirizzi è riservata al Dirigente scolastico, al DSGA e al personale amministrativo della segreteria.
Sono invece a disposizione delle insegnanti indirizzi mail scolastici per ciascun plesso:
SCUOLA PRIMARIA di Cirimido :
SCUOLA PRIMARIA di di Fenegrò:
SCUOLA PRIMARIA di: Limido Comasco :
SCUOLA PRIMARIA di: Lurago Marinone :

Le credenziali di accesso devono essere custodite dalle responsabili di plesso e comunicate esclusivamente ai docenti del plesso che ne facciano richiesta.
L'uso personale e non scolastico delle web mail è vietato e sanzionato con l'interdizione dall'uso delle stesse.

Le responsabili di plesso (o docenti da esse personalmente delegate) devono controllare periodicamente le caselle di posta, vigilare sull'uso che ne viene fatto.

3.4 Blog

Un blog è un particolare tipo di sito web che può essere assimilato a un diario personale o a un giornale: uno o più autori scelgono un tema e lo argomentano o pubblicano il resoconto di fatti accaduti. Attualmente la nostra scuola non possiede un Blog. Qualora l'Istituto decidesse di aprire un blog, il TID avrà cura di aggiornare il presente documento con un regolamento d'utilizzo.

3.5 Sito web della scuola

Il sito scolastico è stato ristrutturato completamente nel 2014 ed ha i seguenti parametri:
Dominio : www.comprensivofenegro.gov.it

Il sito scolastico viene tempestivamente aggiornato secondo le norme vigenti sulla trasparenza e in particolare:

- La pubblicazione delle informazioni e delle circolari nella Homepage, nell'Albo on line e nell'Amministrazione Trasparente è a cura del personale di segreteria.
- Le altre sezioni e la struttura stessa del sito vengono aggiornate annualmente o periodicamente dal Webmaster secondo necessità.
- L'accesso alla sezione amministrativa del sito scolastico è riservata al Dirigente Scolastico, al personale di segreteria e al Webmaster, con utenze diversificate.
- L'accesso alla parte pubblica del sito è libera.
- Alcune informazioni possono essere tenute riservate in sezioni protette del sito, accessibili agli utenti dell'Istituto tramite registrazione da effettuarsi previa richiesta scritta alla segreteria .

3.6 Social network

È vietato al personale scolastico e agli alunni di accedere a social network e chat attraverso le strumentazioni della scuola, se non per uso didattico.
In caso di progetti che ne prevedano l'uso, il docente è tenuto a comunicarlo preventivamente al Dirigente Scolastico e a monitorare gli alunni affinché ne facciano un uso corretto, secondo le disposizioni dell'insegnante. È comunque vietato pubblicare sui social network o su qualunque sito internet documenti, foto, registrazioni audio-video che possano essere lesivi per la reputazione o per la privacy degli alunni e del personale scolastico.
Segnalazioni di infrazioni possono essere comunicate secondo il protocollo presente al capitolo 5.

3.7 Registro scolastico

Il registro elettronico on line è uno strumento al quale possono accedere tutti i membri della Comunità Scolastica, previa registrazione da parte della segreteria. Tutti gli utenti devono essere provvisti di nome utente e password.
L'uso del registro è personale e riservato: ogni utente deve provvedere affinché i dati di login restino riservati e si impegna a cambiare password nel caso in cui la riservatezza degli stessi sia stata violata.

a) ***Area Amministrativa***

Il Dirigente scolastico, il personale di segreteria e l'Amministratore del registro possono accedere a specifiche aree riservate, personalizzate secondo ruoli e mansioni stabilite, per configurare le impostazioni di sistema e inviare comunicazioni al personale.

b) ***Area Docenti***

Il personale scolastico può accedere solo all'area riservata ai docenti.
I dati di accesso all'account devono essere richiesti personalmente all' Amministratore del registro o in segreteria.
Il personale scolastico:

- È tenuto a leggere le comunicazioni ufficiali della segreteria.
- Può inviare comunicazioni e avvisi ai genitori tramite l'apposita sezione.
- Può pubblicare e condividere con docenti e alunni materiale didattico.
- Deve registrare quotidianamente le presenze e firmare il registro di classe .
- Deve tenere periodicamente aggiornate le sezioni riguardanti la Programmazione e i voti.
- Deve compilare le proposte di voto e i documenti di valutazione entro i termini previsti per lo scrutinio.
- Deve comunicare alla segreteria eventuali incongruenze nell'elenco degli alunni .
- Deve segnalare all'Amministratore del registro eventuali anomalie nel funzionamento.

c) ***Area Tutori***

I genitori (tutori) accedono all'apposita sezione ad essi riservata ed hanno a disposizione due account diversificati (uno per genitore).
I dati di accesso all'account vengono consegnati personalmente ai genitori delle classi prime della scuola secondaria .
I genitori, non presenti in tale occasione o i genitori di alunni trasferiti in corso d'anno, devono richiedere i dati di accesso in segreteria e ritirarli personalmente.
I genitori:

- Sono tenuti a leggere le comunicazioni ufficiali della segreteria e dei docenti.
- Devono controllare quotidianamente il registro, in particolare le assenze, i voti, le note, i documenti di valutazione e l'agenda di classe.
- Possono effettuare le prenotazioni dei colloqui con i docenti
- Possono rispondere alle comunicazioni del personale docente.
- Possono compilare personalmente la sezione con i dati anagrafici.
- Devono comunicare alla segreteria eventuali incongruenze nei dati anagrafici personali o del proprio figlio.
- Devono segnalare ai docenti eventuali anomalie nel funzionamento o incongruenze nei dati inseriti.

- Devono mantenere riservati i dati di accesso.

3.8 Protezione dei dati personali

Si ricorda a tutto il personale scolastico che il segreto professionale o d'ufficio obbliga a non rivelare le informazioni aventi natura di segreto, secondo un codice etico (legato al rispetto della persona), deontologico (come norma di comportamento professionale) e giuridico.
È conseguentemente vietato al personale scolastico di divulgare personalmente o di pubblicare su blog, social network o siti personali qualunque informazione possa violare il segreto d'ufficio.

a) ***Procedure operative per la protezione dei dati personali.***

Per quanto riguarda dati di accesso a strumentazioni, reti wi-fi o registri, tutti i dipendenti devono:

- Custodire i dati di accesso facendo attenzione che terzi non ne vengano a conoscenza.
- Nel caso in cui sia violata la segretezza di una password, il personale deve provvedere alla sua immediata sostituzione (nel caso di password personale) o alla repentina comunicazione al personale responsabile (nel caso di password condivise impostate dall'Amministratore della rete).

Il personale scolastico, nello svolgimento delle proprie mansioni, deve prestare particolare attenzione a:

- Non divulgare ad estranei le informazioni di cui viene a conoscenza durante il servizio.
- Non fare copie, per uso personale, dei dati sensibili.
- Osservare i criteri di riservatezza.
- Trattare i dati in modo lecito e secondo correttezza.
- Trattare i dati per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati.
- Comportarsi nel pieno rispetto delle misure minime di sicurezza, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione, di perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Il personale di segreteria è inoltre tenuto a:

- Provvedere al salvataggio di bakup periodici (almeno settimanali) su supporti esterni che dovranno essere opportunamente conservati e non accessibili a persone non autorizzate
- Adottare delle cautele nella trasmissione, nella riproduzione e nella distruzione dei documenti contenenti dati personali, al fine di prevenire eventuali rischi di accesso ai dati da parte di soggetti non autorizzati.
- Per tutte le procedure inerenti la sicurezza e la gestione dei dati fare riferimento ai documenti interni previsti dalle norme.

L'Amministratore di rete, il Webmaster, l'Amministratore del sito e l'Assistente tecnico, che possiedono dati di accesso a reti, siti, registri, strumentazioni per lo svolgimento delle specifiche mansioni, sono inoltre tenuti a:

- Non comunicare a persone non autorizzate i dati di accesso di terzi in loro possesso
- Non utilizzare i dati di accesso di terzi senza motivata ragione

4. STRUMENTAZIONE

PERSONALE 4.1 Studenti

Non è consentito l'uso di dispositivi personali (notebook, tablet, cellulare, ecc …), fatta eccezione per gli alunni con DSA o diversamente abili per i quali ci sia evidenza di averne necessità per un uso strettamente didattico o per la comunicazione: in questo caso i genitori dovranno farne richiesta scritta documentata al Dirigente. I team o i Consigli di classe successivamente provvederanno ad approvare o a respingere la richiesta con propria decisione motivata.
Viceversa, i team o i consigli di classe potranno promuovere, per gli alunni per i quali ci sia evidenza che l'uso di dispositivi personali possa migliorare il percorso didattico e rimuovere ostacoli all'apprendimento, con la condivisione delle famiglie, l'uso di device personali.
L'uso di dispositivi personali (notebook, tablet, cellulare, ecc …), finalizzato a singole attività, può comunque essere autorizzato dai docenti e sotto la loro responsabilità. L'Istituto non sarà comunque ritenuto responsabile in caso di furto o danneggiamento accidentale.
In tal caso, l'uso delle strumentazioni personali e l'accesso ad internet è regolato dalle norme al capitolo 3.2; inoltre, nell'edificio scolastico e nell'area di pertinenza, è vietato registrare foto, video e audio con dispositivi digitali personali se non con l'autorizzazione dei docenti e per attività programmate. Non è comunque consentito l'uso del cellulare a scuola per l'invio e la ricezione di messaggi (SMS, MMS, ecc) e telefonate personali, né per l'accesso ad internet e alle piattaforme Social (Facebook, Whatsapp, ecc...).
In caso di uscite didattiche, viaggi d'istruzione, recite, progetti sul territorio ed altre situazioni affini, valgono le stesse regole delle normali attività didattiche. Tuttavia, i docenti accompagnatori potranno comunicare agli alunni e ad eventuali genitori presenti, quali dispositivi digitali sono consentiti (cellulari, macchine fotografiche, videocamere, Ipad, Ipod...) e le regole di utilizzo. L'Istituto non sarà ritenuto responsabile in caso di furto o danneggiamento accidentale.
Le foto e i video eventualmente registrati in queste occasioni, dietro autorizzazione dei docenti, dovranno avere un uso personale e non potranno essere diffusi in rete qualora siano state riprese terze persone (altri alunni, genitori, docenti ed operatori).

4.2 - Docenti

È consentito l'uso di strumentazioni personali (notebook, tablet…) per attività didattiche o extracurricolari, ma l'Istituto non sarà ritenuto responsabile in caso di furto o danneggiamento accidentale.
L'uso di internet per fini personali, attraverso dispositivi privati, non è consentito durante l'orario di servizio; è invece consentito al di fuori dell'orario di servizio, nel rispetto dei diritti della cittadinanza digitale e delle norme vigenti di utilizzo legale della rete.
Non è, comunque, consentito l'acceso ad internet attraverso la rete scolastica per fini personali.
Non è consentito l'uso del cellulare durante l'orario di servizio se non per attività didattiche.

In caso di viaggi d'istruzione, recite, progetti sul territorio ed altre situazioni affini, i docenti accompagnatori possono utilizzare dispositivi digitali personali per

effettuare foto e video che non potranno comunque essere pubblicati in rete attraverso social network o siti internet.

4.3 - Personale amministrativo e i collaboratori scolastici

Per garantire la sicurezza dei dati sensibili, non è consentito svolgere attività amministrativa su dispositivi informatici personali (notebook, tablet...).
Non è, comunque, consentito l'acceso ad internet attraverso la rete scolastica per fini personali.
Non è, inoltre, consentito l'uso del cellulare per fini personali durante l'orario di servizio.

4.4 – Altri operatori

Tutti gli altri operatori presenti a qualsiasi titolo nella scuola (esperti esterni, collaboratori, ditte esterne...) dovranno attenersi alle norme previste per il personale scolastico.

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI

CASI 5.1 – Prevenzione

La prevenzione, invece, è lo strumento più efficace per proteggere i minori dai pericoli online.
Per questo è importante che i giovani imparino a valutare criticamente i contenuti, riconoscano i possibili rischi e sappiano come proteggersi. I genitori e gli insegnanti svolgono un'importante funzione di accompagnamento in questo contesto, in qualità di interlocutori di fiducia pronti a condividere esperienze e ad intervenire attivamente se necessario.

a) Rischi

Il problema della sicurezza on line non è riconducibile esclusivamente all'esistenza di atti criminali, più o meno conosciuti e insidiosi, di cui i ragazzi possono cadere vittima, ma anche alla possibilità che l'utilizzo di tali strumenti tecnologici, nell'arco della giornata di un ragazzo, cominci a prevalere a scapito di spazi di aggregazione concreti, attività sociali, ricreative e sportive.

I rischi più comuni in rete sono rappresentati da:
· Adescamento Online
· Cyberbullismo
· Happy slapping
· Sexting
· Violazione della Privacy
· Accesso a contenuti non adeguati
· Dipendenza da Internet
· Gioco d'azzardo e siti di realtà virtuale

Per approfondimenti sui rischi legati all'uso delle nuove tecnologie è possibile consultare l'allegato 5 "Vademecum"

b) Azioni per la riduzione dei rischi

L'Istituto si prefigge di intraprendere le seguenti azioni per la prevenzione dei rischi on line:

- Monitorare la realtà dell'istituto, tramite un questionario, per ridurre il grado di rischio relativo ad eventi problematici *(in particolare violazione della Privacy, Cyberbullismo, Accesso a contenuti non adeguati)*
- Sensibilizzare la Comunità Scolastica al problema dei rischi legati ad un uso non responsabile di internet *con un incontro informativo per i genitori*
- Promuovere progetti per la responsabilizzazione degli alunni in qualità di Cittadini Digitali
  Insegnando agli alunni ad essere responsabili nell'uso dei dispositivi digitali, forniamo loro un essenziale strumento sia per proteggersi da situazioni a rischio, sia per evitare di diventare loro stessi cyber bulli.
  - *Avvalersi del supporto e della collaborazione dell'ASCI(psicologia scolastica, servizio di prevenzione, ASCI-LINK) e dei servizi sociali e/o associazioni presenti sul territorio.*

5.2 - Rilevazione

a) Che cosa segnalare

Il personale scolastico è tenuto a segnalare situazioni potenzialmente a rischio di bullismo e cyber bullismo.

Gli alunni e i genitori possono segnalare:

- Casi di cyberbullismo, adescamento on line, happy slapping, sexting , violazione della Privacy , accesso a contenuti non adeguati, dipendenza da internet e qualunque altra situazione di rischio effettiva, anche se accadute in ambito extrascolastico.

b) Come segnalare e a chi

Gli alunni possono effettuare personalmente le loro segnalazioni a qualunque docente dell'Istituto, anche in forma riservata, o allo sportello d'ascolto presso la scuola secondaria (le modalità di accesso allo sportello vengono delineate agli alunni all'inizio di ogni anno scolastico).
I genitori possono effettuare le loro segnalazioni personalmente ai docenti di classe, alla vicepreside, al Dirigente Scolastico, o allo sportello di ascolto presso la scuola secondaria. Le modalità di contatto vengono annualmente delineate all'inizio di ogni anno scolastico.
Il Dirigente Scolastico potrà, comunque, essere contattato telefonicamente o tramite la e-mail istituzionale, anche al solo scopo di fissare un appuntamento.
I docenti sono tenuti ad effettuare le segnalazioni al DS e a coinvolgere il team/consiglio di classe e l'Animatore Digitale.
Il Dirigente scolastico, monitorata la situazione, potrà richiedere una relazione scritta su quanto accaduto ed eventualmente allertare gli operatori di polizia laddove sia necessario

La collaborazione scuola-famiglia è di vitale importanza al fine di promuovere un uso consapevole dei nuovi media e quindi oltre a condividere informazioni sulla sicurezza in rete, sul suo corretto utilizzo e sui potenziali pericoli è necessario anche informare circa possibili strategie di intervento qualora si rilevassero abusi. La linea di ascolto 1.96.96 (attiva 24 ore su 24, 365 giorni all'anno) e la chat (attiva tutti i giorni dalle 8.00 alle 22.00 (sabato e domenica dalle 8.00 alle 20.00) di Telefono Azzurro accolgono qualsiasi richiesta di ascolto e di aiuto da parte di bambini/e e

ragazzi/e fino ai 18 anni o di adulti che intendono confrontarsi su situazioni di disagio/pericolo in cui si trova un minorenne.
Il servizio di helpline è riservato, gratuito e sicuro, dedicato ai giovani o ai loro familiari che possono chattare, inviare e-mail o parlare al telefono con professionisti qualificati relativamente a dubbi, domande o problemi legati all'uso delle nuove tecnologie digitali e alla sicurezza online. Inoltre, è disponibile il 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.
Anche la Polizia Postale e delle Comunicazioni è attualmente impegnata in diverse attività a sostegno della navigazione protetta dei minori ed è competente a ricevere segnalazioni su qualsiasi tipo di reato informatico.

c) Come gestire le segnalazioni.

In caso di segnalazione da parte di un alunno o di un genitore, o su sollecitazione del DS (nel caso la segnalazione sia pervenuta direttamente al DS), i docenti sono tenuti a:

- Approfondire l'accaduto attraverso uno o più colloqui, possibilmente riservati, con le persone coinvolte
- Verificare, nei limiti del possibile, che quanto segnalato sia realmente accaduto
- Seguire il protocollo per la gestione dei casi (per una gestione condivisa del problema)

d) Procedure operative per la rilevazione, la gestione il monitoraggio delle segnalazioni

Quanto delineato nei punti a), b) e c), insieme agli allegati 1, 2, 3 e 5 costituiscono le procedure operative per la rilevazione e le gestione delle segnalazioni.

Il monitoraggio delle segnalazioni verrà tenuta dal DS, o da suo delegato, tramite la tenuta del diario di bordo (all. 4)

5.3 - Gestione dei casi

a) Definizione delle azioni da intraprendere a seconda della specifica del caso

Intervenire in situazioni di cyberbullismo/sexting/adescamento on line non è mai semplice: spesso si pensa di non sapere esattamente cosa fare e si ha timore di essere inadeguati.

Nei casi in cui invece si ha un'idea teorica di come si potrebbe agire, il timore può invece essere quello di non avere i tempi e gli strumenti adeguati.
L'importante è non agire in solitudine e, soprattutto, non fare scelte improvvisate, magari sull'onda delle emozioni del momento, sulle azioni da intraprendere.
I docenti, pertanto, avuta notizia di un caso (dagli alunni, dai genitori o da qualsiasi altra fonte) e seguite le indicazioni del punto c) del paragrafo 5.2, prima di intraprendere qualsiasi azione, sottoporranno la questione al Dirigente Scolastico e/o all'Animatore Digitale e si confronteranno successivamente con il team/Consiglio di Classe.
Successivamente, sulla scorta degli strumenti delineati al successivo punto b), che descrivono la sequenza delle possibili azioni da intraprendere, e in accordo con il Dirigente Scolastico, l'animatore Digitale e il team/consiglio di classe, si deciderà il percorso da seguire e se ne terrà traccia.

L'obiettivo a lungo termine della comunità scolastica è quello di creare una memoria condivisa non solo di ciò che accade nella scuola rispetto al web, ma anche di strutturare una fonte esemplificativa che possa orientare sempre più e sempre meglio le azioni di contrasto ad episodi che, nel tempo, potrebbero ripetersi.

b) Procedure operative per la gestione dei casi.

Procedure operative per la gestione dei casi:

In allegato sono presenti alcuni strumenti operativi che delineano i percorsi da intraprendere in funzione del singolo caso. La loro funzione è agevolare:

- nel decidere come intervenire;
- nel tenere traccia di ciò che è avvenuto rispetto ai comportamenti degli alunni online e di come è stato gestito.

cyberbullismo (allegato1)
sexting (allegato 2)
adescamento on line (allegato 3)
Per tenere traccia di ciò che è avvenuto (allegato 4: diario di bordo scuola).

Per le eventuali sanzioni a carico degli alunni, si rimanda al regolamento d'Istituto

La presente policy è stata redatta sulle linee guida fornite dal portale Generazioni Connesse.