ISTITUTO OMNICOMPRENSIVO DI GUGLIONESI

Via Cristoforo Colombo 6 | 86034 GUGLIONESI (CB)
Telefono +039 0875 689006 | Fax +039 0875 681769
Email: cbpm01000c@istruzione.it | cbpm01000c@pec.istruzione.it
Sito: www.omnicomprensivoguglionesi.gov.it

E-SAFETY POLICY

[1] Revisione a.s. 2017/2018

1. INTRODUZIONE

Il presente documento è elaborato tenendo conto dei seguenti atti e documenti:

- la Legge n. 71 del 29 maggio 2017;
- l' "*Aggiornamento delle LINEE DI ORIENTAMENTO per la prevenzione e il contrasto del cyberbullismo*", pubblicate dal MIUR nel mese di ottobre 2017;
- le "*LINEE DI ORIENTAMENTO per azioni di prevenzione e di contrasto al bullismo e al cyberbullismo*", pubblicate dal MIUR nel mese di aprile 2015;
- il piano d'azione elaborato dalla scuola nell'ambito del progetto "*Generazioni Connesse*", coordinato dal MIUR e sostenuto dalla Commissione Europea.

Esso ha lo scopo di definire:

- ✧ l' approccio della scuola alle tematiche legate alle competenze digitali, alla sicurezza online e ad un uso positivo delle tecnologie digitali nella didattica;
- ✧ le norme comportamentali e le procedure per l'utilizzo delle tecnologie dell'informazione e della comunicazione (ICT) in ambiente scolastico;
- ✧ le misure per la prevenzione;
- ✧ le misure per la rilevazione e gestione delle problematiche connesse a un uso non consapevole delle tecnologie digitali.

"Le studentesse e gli studenti devono essere sensibilizzati ad un uso responsabile della Rete e resi capaci di gestire le relazioni digitali in *agorà* non protette. Ed è per questo che diventa indispensabile la maturazione della consapevolezza che Internet può diventare, se non usata in maniera opportuna, una pericolosa forma di dipendenza. Compito della Scuola è anche quello di favorire l'acquisizione delle competenze necessarie all'esercizio di una cittadinanza digitale consapevole. Responsabilizzare le alunne e gli alunni significa, quindi, mettere in atto interventi formativi, informativi e partecipativi"[2].

La E-Safety Policy è da intendersi quale strumento flessibile e suscettibile di periodici aggiornamenti, in grado di rispondere alle sfide educative e pedagogiche derivanti dall'evolversi costante e veloce delle nuove tecnologie.
Essa potrà, quindi, essere periodicamente revisionata.

[2] "*Aggiornamento delle LINEE DI ORIENTAMENTO per la prevenzione e il contrasto del cyberbullismo*", MIUR ottobre 2017.

2. FORMAZIONE E CURRICOLO

Il Piano Triennale dell'Offerta Formativa (PTOF) della scuola, coerentemente con la Legge 107 del 2015 e con il Piano Nazionale Scuola Digitale (PNSD) del MIUR, ha individuato, tra gli obiettivi formativi prioritari da sviluppare nell'arco del triennio, lo sviluppo delle competenze digitali degli studenti, con particolare riguardo al pensiero computazionale, all'utilizzo critico e consapevole dei social network e dei media nonché alla produzione e ai legami con il mondo del lavoro.

Il curricolo scolastico prevede, quindi, il potenziamento delle competenze digitali degli studenti: "saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione per il lavoro, il tempo libero e la comunicazione…, l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet"[3].

In questo senso le TIC (Tecnologie dell'Informazione e della Comunicazione) preparano gli studenti ad un'attiva e consapevole partecipazione ad un mondo in rapida evoluzione e nel quale è necessario acquisire abilità e competenze in grado di facilitare l'adattamento dell'individuo ai continui cambiamenti.

Si rende quindi necessario lo sviluppo e la diffusione di una mentalità tecnologica diffusa e precoce, intesa come alfabetizzazione al senso, all'utilizzabilità in contesti dati e per scopi definiti da un lato ed acquisizione sempre più consapevole di strategie efficaci per il dominio di una macchina complessa che impiega e genera oggetti immateriali, dall'altro.

Gli alunni dovrebbero imparare ad utilizzare le TIC per cercare, esplorare, scambiare e presentare informazioni in modo responsabile, creativo e con senso critico ed essere in grado di avere un rapido accesso a idee ed esperienze provenienti da persone, comunità e culture diverse. Alla scuola spetta quindi anche il compito di trovare raccordi efficaci tra la crescente dimestichezza degli alunni con le Tecnologie dell'Informazione e della Comunicazione e l'azione didattica quotidiana.

Le TIC possono infatti offrire significative occasioni per sviluppare le competenze di comunicazione, collaborazione e problem solving.

3. STRATEGIE E MISURE

Le strategie previste dalla scuola per garantire la sicurezza in rete sono le seguenti:

- percorsi di formazione per un uso consapevole delle TIC rivolti agli insegnanti;
- percorsi di formazione per un uso consapevole delle TIC rivolti agli studenti;
- coinvolgimento dei genitori come partner educativi nei percorsi di formazione che riguardano gli studenti;
- controllo del sistema informatico (cronologia, cookies, ecc.) da parte dei responsabili;
- installazione di firewall sull'accesso Internet;
- presenza di un docente o di un adulto responsabile durante l'utilizzo di Internet, della piattaforma o di altre TIC da parte degli studenti;
- aggiornamento periodico del software antivirus e scansione delle macchine in caso di

[3] Raccomandazione del Parlamento europeo e del Consiglio del 18 dicembre 2006 (2006/962/CE).

sospetta presenza di virus;
- utilizzo di penne USB, CD/DVD o altri dispositivi esterni personali, solo se autorizzati.

Ciascun utente connesso alla rete deve:
- rispettare la legislazione vigente e la presente policy;
- tutelare la propria privacy, quella degli altri utenti adulti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni elettroniche cui ha accesso;
- rispettare la *netiquette* (regole condivise che disciplinano il rapportarsi fra utenti della rete, wiki, siti, forum, mail e di qualsiasi altro tipo di comunicazione).

4. RUOLI E RESPONSABILITÀ

Il docente può avvalersi, durante l'attività didattica, di diversi strumenti, quali PC, LIM, tablet e device degli studenti (B.Y.O.D.) e deve:
- utilizzare le TIC e la rete Internet per le attività didattiche ed educative degli studenti;
- controllare l'uso delle tecnologie digitali, dei dispositivi mobili e fissi da parte degli studenti durante le attività didattiche;
- illustrare ai propri alunni le regole di utilizzo contenute nel presente documento;
- dare chiare indicazioni sul corretto utilizzo della rete, condividendo con gli alunni la *netiquette* e indicandone le regole;
- segnalare prontamente eventuali malfunzionamenti o danneggiamenti all'assistente tecnico;
- non divulgare le credenziali di accesso agli account (username e password) e alla rete wifi;
- non allontanarsi dalla postazione lasciandola incustodita, se non prima di aver effettuato la disconnessione;
- non salvare sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili;
- nelle attività didattiche in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei.

Gli alunni sono tenuti a:
- utilizzare le TIC su indicazioni del docente;
- accedere all'ambiente di lavoro con il corretto account, non divulgandone le credenziali di accesso (username, password);
- comunicare immediatamente all'insegnante eventuali malfunzionamenti della strumentazione e/o contatto accidentale con informazioni, immagini e/o applicazioni inappropriate;
- non eseguire tentativi di modifica della configurazione di sistema delle macchine;
- non utilizzare la strumentazione della scuola a scopi personali, ludici e/o ricreativi (a meno che l'attività didattica non lo preveda esplicitamente);
- non utilizzare propri dispositivi esterni personali senza aver acquisito il permesso da parte dell'insegnante;
- chiudere correttamente la propria sessione di lavoro.

Ai genitori, in qualità di partner educativi, si chiede di:

- sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle Tecnologie dell'Informazione e delle Comunicazioni nella didattica;
- concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di Internet;
- 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.

5. GESTIONE DELL'INFRASTRUTTURA DELLA SCUOLA

a) Accesso ad Internet

L'accesso alla rete Internet della scuola è protetto da un firewall e da password, una per ciascun fruitore. Ogni utente dovrà, pertanto, avere cura di disconnettere il proprio accesso al termine del suo utilizzo.
I computer portatili collocati nelle aule accedono ad internet attraverso la rete LAN/WLAN. Nel laboratorio informatico e nelle aule TEAL sono presenti computer portatili e fissi. Tutti i computer presenti nella scuola devono installare un antivirus.
Gli studenti possono accedere ad Internet solo in occasione di attività didattiche o di attività ricreative autorizzate.

b) Sito web della scuola

La scuola utilizza il sito web www.omnicomprensivoguglionesi.gov.it per comunicare a studenti, famiglie, docenti, personale, cittadini e stakeholders del territorio, le informazioni relative all'Istituto, al mondo della Scuola e alla formazione in generale.
Il sito presenta e racconta la scuola e la sua identità, promuovere l'Offerta Formativa dell'Istituto, rende pubblica e trasparente l'attività dell'Istituto, facilita la comunicazione interna ed esterna, offre servizi e strumenti didattici agli alunni e ai docenti, offre servizi e informazioni alle famiglie, promuove una cultura collaborativa, organizzativa e partecipativa.
La scuola nomina il Gestore del sito web, con i seguenti compiti: curare la pubblicazione e l'aggiornamento dei dati e del materiale di valenza formativa e didattica; controllare la qualità dei contenuti e la loro rispondenza agli standard formativi ed educativi della scuola; fornire consulenza e supporto per l'utilizzo del sito web della scuola; gestire le aree riservate del sito.

c) Blog, classi virtuali, piattaforme di condivisione

Coerentemente con quanto riportato nel paragrafo 2 del presente documento, la scuola incentiva l'utilizzo di blog didattici, di classi virtuali e di piattaforme di condivisione, in quanto stimolano la crescita cognitiva comune, l'apprendimento cooperativo, l'acquisizione di competenze nell'uso degli strumenti di comunicazione on line e di tecniche comunicative, il senso di responsabilità.
Responsabile di ciascun ambiente è il docente che lo attiva/utilizza e cura la pubblicazione dei contenuti.

6. USO DI STRUMENTAZIONE PERSONALE

Gli studenti possono utilizzare i propri dispositivi durante le attività didattiche ed accedere alla rete attraverso i dispositivi della scuola solo previa autorizzazione dell'insegnante presente in aula e comunque per finalità didattiche o per attività creative/ricreative preventivamente autorizzate.
I docenti possono utilizzare i dispositivi della scuola per realizzare tutte le attività connesse alla funzione docente. E' consentito ai docenti l'uso dei propri dispositivi in classe per quanto attiene l'attività didattica qualora siano necessari, ma non per questioni personali.

7. CONDIVISIONE E COMUNICAZIONE DELLA POLICY

La E-Safety Policy è pubblicata sul sito della scuola.
La scuola promuove eventi e/o dibattiti informativi e formativi, rivolti a tutto il personale, agli alunni e ai loro genitori, eventualmente anche con il coinvolgimento di esperti, sui temi oggetto di questo Documento.
Allo scopo di condividere regole comuni per l'utilizzo sicuro di Internet sia a casa che a scuola, si invitano i docenti, gli studenti e i genitori a prestare la massima attenzione ai principi e alle regole contenute nel presente documento.

8. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

La scuola pone attenzione alla rilevazione di rischi connessi alla navigazione sul web, in modo particolare:

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

La scuola mette in atto interventi tesi a sensibilizzare gli alunni verso un uso responsabile e consapevole della rete, al fine di assicurare loro il rispetto del diritto ad essere tutelati da abusi e violenze da un lato e, allo stesso tempo, suscitare atteggiamenti di rispetto nei confronti degli altri utenti. Le nuove tecnologie si pongono quale strumento attraverso cui sviluppare pratiche di collaborazione tra gli studenti per riconoscere e accettare la diversità e favorire la partecipazione finalizzata alla costruzione dei diversi percorsi formativi a cui sono chiamati tutti gli alunni.
Qualora i docenti si trovino di fronte a situazioni di criticità, dovranno segnalare tempestivamente quanto rilevato alla Dirigenza Scolastica, che provvederà ad attivare le azioni opportune.

Salvo che il fatto costituisca reato, il Dirigente scolastico che venga a conoscenza di atti di cyberbullismo ne informa tempestivamente i soggetti esercenti la responsabilità genitoriale ovvero i tutori dei minori coinvolti e attiva adeguate azioni di carattere educativo.

9. PROTEZIONE DEI DATI PERSONALI

In generale, l'utente può navigare sul sito web della scuola senza fornire alcun tipo di informazione personale.
L'Istituto Omnicomprensivo di Guglionesi rispetta la privacy dei propri utenti e si impegna a proteggere i dati personali che gli stessi conferiscono all'Istituto in conformità alla normativa vigente.
La scuola raccoglie i dati personali dell'utente in occasione della registrazione per assegnare un codice utente e una password, per emettere un account, necessari all'utente stesso per usufruire di determinati prodotti o servizi offerti dalla scuola. In particolare la registrazione è necessaria all'utente per poter accedere alla aree Riservate, per poter inviare messaggi ad altri iscritti, per inserire commenti alle notizie, quando l'utente chiede di ricevere determinate e-mail o di essere inserito in una mailing-list, o quando l'utente, per qualsiasi altra ragione, comunica i propri dati all'Istituto .
L'Istituto usa tali informazioni solamente ove le stesse siano state legittimamente raccolte in conformità alla presente Policy e nel rispetto della normativa vigente.

10. APPLICAZIONE DELLA E-SAFETY POLICY E GESTIONE DELLE INFRAZIONI

La scuola individua un docente referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo e di supporto al dirigente scolastico per la revisione/stesura della E-policy, dei Regolamenti e dei documenti (PTOF, PdM, ecc.).
Il Dirigente scolastico ha la facoltà di revocare l'accessibilità temporanea o permanente ai laboratori informatici e/o all'utilizzo di strumenti tecnologici (pc, tablet, notebook, ecc) a chi non si attiene alle regole stabilite.
La E-Safety Policy è integrata dai seguenti documenti:

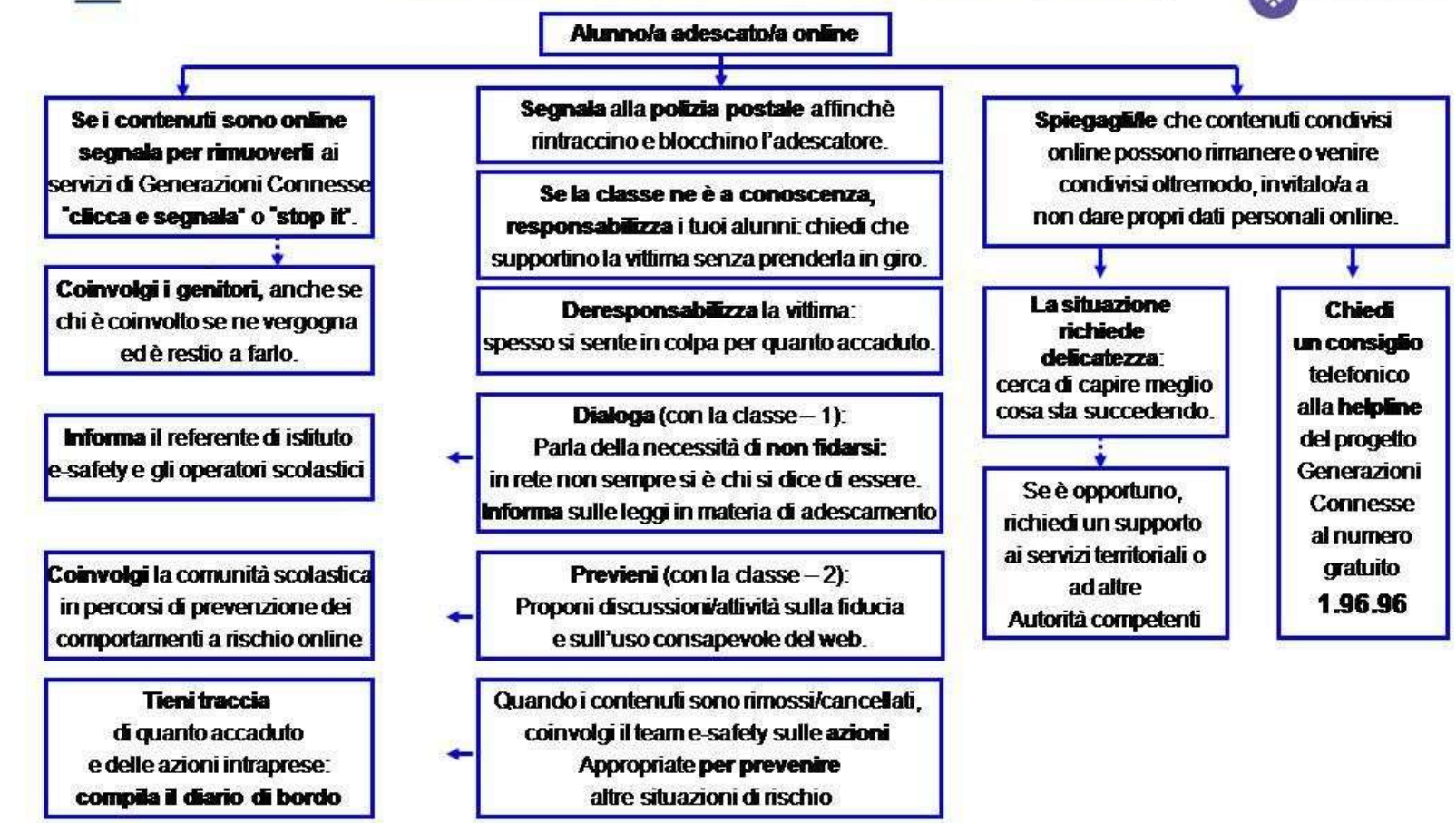
- Regolamento laboratori di informatica,
- Regolamento aule TEAL,

che costituiscono sezioni del Regolamento di Istituto.

Si allegano al presente documento le schede operative fornite dalla piattaforma "Generazioni connesse" per la rilevazione e la gestione dei casi.

Sicurezza in rete - Schema per la scuola

Cosa fare in caso di.... adescamento online? (P SU AN)



Sicurezza in rete - Schema per la scuola

Cosa fare in caso di.... cyberbullismo?

Alunno/a preso in giro/minacciato/offeso online

Dialoga (con la classe - 1):
Parla del cyberbullismo e delle sue conseguenze (non nominare gli alunni coinvolti). Insegna loro a **chiedere aiuto** per situazioni di questo tipo.

Dialoga (con la classe - 2):
Chiedi agli alunni coinvolti di intervenire per far terminare le prese in giro: il loro silenzio asseconda quanto sta accadendo.

Parla della necessità di **non diffondere** ulteriormente online i materiali.

Informa gli alunni su ciò che dice la **legge italiana** sul cyberbullismo, che è reato.

Previeni (con la classe - 3):
Proponi attività in classe sull'empatia e sul riconoscimento delle emozioni (proprie e altrui)

Quando il cyberbullismo termina, coinvolgi il team e-safety sulle **azioni** appropriate per prevenire altre situazioni di rischio

Se gli alunni coinvolti sono d'accordo, **informa** i genitori

Coinvolgi il referente di istituto dell'e-safety e gli operatori scolastici su quanto sta accadendo

Segnala alla **polizia postale** [segnala: a) contenuto b) modalità di diffusione].

Coinvolgi la comunità scolastica in percorsi di prevenzione dei comportamenti a rischio online

Tieni traccia di quanto successo e delle azioni intraprese: **compila il diario di bordo**

La situazione richiede delicatezza: cerca di capire meglio cosa sta succedendo.

Se è opportuno, richiedi un sostegno ai servizi territoriali o ad altre Autorità competenti (soprattutto se il cyberbullismo non si limita alla scuola)

Chiedi un consiglio telefonico alla **helpline** del progetto Generazioni Connesse al numero gratuito **1.96.96**

Sicurezza in rete - Schema per la scuola

Cosa fare in caso di.... sexting?

Alunno/a invia o riceve foto o video sessualmente espliciti

Se foto/video sono online, segnala per rimuovere ai servizi di Generazioni Connesse **"clicca e segnala"** o **"stop it"**. Valuta il coinvolgimento della **polizia postale** [segnala: a) contenuto b) modalità di ricezione/invio].

Dialoga (con la classe - 1): chiedi di non prendere in giro il compagno/a per quanto successo; spiega che possesso (e non solo diffusione) di tali materiali è reato.

Informa i ragazzi su ciò che dice la **legge italiana** sulla diffusione di Materiale pedopornografico (reato)

Dialoga (con la classe - 2): Proponi una riflessione sulle relazioni online

Previeni – (con la classe - 3): Proponi attività in classe su fiducia e su affettività

Quando i contenuti sono rimossi/cancellati, coinvolgi il team e-safety sulle **azioni** appropriate **per prevenire** altre situazioni di rischio

Se li ha ricevuti, spiega che contenuti condivisi online possono rimanere lì o venire condivisi oltremodo, invitalo/a a chiedere di cancellarli e, se no, a segnalarli.

Lavora con i coinvolti perché accettino il **coinvolgimento dei genitori** (spesso se ne vergognano).

Informa il referente di istituto e-safety e gli operatori scolastici.

Coinvolgi la comunità Scolastica in percorsi di prevenzione dei comportamenti a rischio online

Tieni traccia di quanto accaduto e delle azioni intraprese: **compila il diario di bordo**

Se li ha inviati, spiega che contenuti condivisi online possono rimanere lì o venire condivisi oltremodo, invitalo/a a chiedere di cancellarli e, se no, a segnalarli.

La situazione richiede delicatezza: cerca di capire meglio cosa sta succedendo.

Chiedi un consiglio telefonico alla **helpline** del progetto Generazioni Connesse al numero gratuito **1.96.96**

Se è opportuno, richiedi un supporto ai servizi territoriali o ad altre Autorità competenti