Istituto Comprensivo Statale di Appiano Gentile
Scuola Primaria e Secondaria di 1° grado
Via Cherubino Ferrario, n.4 - Appiano Gentile
Telefono 031/891272
e mail uffici: coic82700g@istruzione.it C.F. 80014000139
Pec: COIC82700G@pec.istruzione.it

E – SAFETY POLICY

Anno scolastico 2019 - 2020

1. Introduzione

1.1 Scopo della Policy
1.2 Ruoli e Responsabilità
1.3 Condivisione e comunicazione della Policy all'intera comunità scolastica
1.4 Gestione delle infrazioni alla Policy
1.5 Monitoraggio dell'implementazione della Policy e suo aggiornamento
1.6 Integrazione della Policy con i Regolamenti esistenti

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

2.1 Accesso ad internet: filtri, antivirus e navigazione
2.2 Gestione accessi
2.3 Sito web della scuola
2.4 Protezione dei dati personali

3. Strumentazione personale

3.1 Strumentazione personale nella comunità scolastica

4. Prevenzione, rilevazione e gestione dei casi

4.1 Prevenzione
4.2 Rilevazione
- Che cosa segnalare
- Come segnalare: quali strumenti e a chi

4.3 Gestione dei casi
- Definizione delle azioni da intraprendere a seconda della specifica del caso.

1. Introduzione

1.1 *Scopo della Policy*

Le tecnologie digitali sono sempre più presenti nella quotidianità e bambini e adolescenti entrano in contatto con esse in età precoce. La presenza di tali tecnologie offre nuove opportunità a livello didattico, ma a esse devono accompagnarsi riflessioni e azioni volte a un utilizzo consapevole, sicuro e positivo, soprattutto da parte dei preadolescenti e adolescenti che delle tecnologie fanno un uso immediato e spesso poco consapevole, proprio in virtù della loro enorme diffusione e della apparente semplicità di utilizzo.

Se bambini e ragazzi mostrano un'innata predisposizione all'uso delle tecnologie, tuttavia, a questa abilità, non sempre corrisponde un'adeguata e corretta capacità interpretativa della mole di informazioni alla quale essi sono di continuo sottoposti, in primo luogo attraverso i social network, i quali, se utilizzati in modo superficiale e inappropriato, possono trasformarsi in veicoli di cyberbullismo.

Il presente documento intende fornire alcune linee guida rispetto alle azioni dell'Istituto in ordine a:

- utilizzo consapevole delle TIC in ambiente scolastico e nella didattica
- prevenzione e gestione di situazioni problematiche connesse all'uso delle tecnologie digitali.

1.2 *Ruoli e responsabilità*

La comunità degli adulti ha un ruolo fondamentale nel garantire l'utilizzo adeguato e sicuro delle tecnologie da parte di bambini e ragazzi; nella tabella sottostante vengono riassunti i ruoli e le responsabilità della comunità scolastica

RUOLO	RESPONSABILITÀ
Dirigente scolastico	• garantire la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri della comunità scolastica; • garantire ai propri docenti una formazione di base sulle TIC, che consenta loro di possedere le competenze necessarie all'utilizzo di tali risorse; • garantire l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza online.
Animatore digitale	• stimolare la formazione interna alla scuola negli ambiti del PNSD, favorendo l'animazione e la partecipazione di tutta la comunità scolastica alle attività formative, come ad esempio quelle organizzate attraverso gli snodi formativi; • individuare soluzioni metodologiche e tecnologiche sostenibili da diffondere all'interno dell'ambiente scolastico
Direttore dei Servizi Generali e Amministrativi	• assicurare, nei limiti delle risorse finanziare disponibili, gli interventi di manutenzione richiesti da cattivo funzionamento e/o danneggiamento della dotazione tecnologica dell'Istituto, controllando al contempo che le norme di sicurezza vengano rispettate; • curare la registrazione di disservizi e delle problematiche relative alla rete e all'uso del digitale segnalate dai docenti, provvedendo all'intervento del personale tecnico di

	assistenza.
Docenti	• illustrare agli alunni le regole contenute nel presente documento; • illustrare agli alunni il regolamento riguardante l'utilizzo di internet, degli strumenti informatici e dei relativi software, i diritti inerenti il copyright; • offrire indicazioni sul corretto utilizzo della rete condividendo la *netiquette* e indicandone le regole; • controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche ecc. durante le lezioni e altre attività che ne prevedano l'uso per scopi didattici ed evitare che gli alunni si connettano a siti inadeguati; • segnalare prontamente malfunzionamenti o danneggiamenti al tecnico informatico o all'Animatore digitale; • provvedere alla propria formazione/aggiornamento sull'utilizzo del digitale, con particolare riferimento alla dimensione etica (tutela della privacy, rispetto della netiquette, lotta al cyberbullismo); • segnalare prontamente alle famiglie le problematiche emerse in classe nell'utilizzo del digitale e stabilire comuni linee di intervento educativo per affrontarle; (?) • segnalare al Dirigente scolastico e ai suoi collaboratori episodi di mancato rispetto delle norme di comportamento stabilite dalla scuola, avviando le procedure previste in caso di violazioni.
Referente cyberbullismo	• essere interfaccia con le Forze di Polizia e con le associazioni presenti sul territorio per il coordinamento delle iniziative di prevenzione e contrasto al cyberbullismo; • coordinare azioni di sensibilizzazione per la diffusione di una cultura sull'uso consapevole delle TIC; • proporre modelli di griglie per l'osservazione e la rilevazione dei segnali precursori di disagio/comportamenti a rischio relativamente all'uso non consapevole della rete; • prevedere, in accordo con il Dirigente, linee di intervento per la gestione e la presa in carico dei casi di abuso o di altre problematiche; • raccogliere e diffondere buone pratiche educative e azioni di monitoraggio; • curare la revisione della Policy.
Personale ATA	• assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso

	improprio o a dannosi attacchi esterni; • acquisire un'adeguata consapevolezza sulla sicurezza informatica, sulla politica dell'Istituto e relative buone pratiche; • segnalare qualsiasi abuso, anche sospetto, al Dirigente scolastico o all'Animatore digitale o al Referente cyberbullismo per le opportune indagini/azioni/sanzioni; • mantenere tutte le comunicazioni digitali con gli alunni e i genitori/tutori a livello professionale e realizzate attraverso i canali scolastici ufficiali.
Alunni	• leggere, comprendere e accettare la E-Policy; • ascoltare e seguire le indicazioni fornite dai docenti per un uso corretto e responsabile delle tecnologie digitali, attuando le regole di e-safety per evitare situazioni di rischio; • chiedere l'intervento dell'insegnante e/o dei genitori nello svolgimento dei compiti a casa per mezzo del digitale qualora insorgano difficoltà o dubbi nel suo utilizzo; • non utilizzare il proprio telefono cellulare e/o altri dispositivi elettronici e di intrattenimento (mp3, ipod, ipad, notebook, fotocamera) durante ogni attività scolastica, in tutti i locali della scuola, salvo specifiche deroghe autorizzate dal docente a integrazione dell'attività scolastica; • tenere i propri dispositivi, se presenti, spenti e opportunamente custoditi negli zaini.
Genitori	• contribuire, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete; • vigilare l'uso dei diversi dispositivi elettronici controllando che ciò avvenga nel rispetto delle norme di sicurezza; • agire in modo concorde con la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite.

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

Al fine di evitare che l'adozione di questa policy sia un puro atto formale, l'Istituto si impegna a mettere in atto una serie di azioni.

Per il personale scolastico:

- discutere negli organi collegiali le norme adottate dalla scuola in materia di sicurezza nell'utilizzo del digitale e rendere note all'intera comunità scolastica tramite pubblicazione del presente documento sul sito web della scuola;
- il personale della scuola riceverà un'adeguata informazione/formazione sull'uso sicuro e responsabile di internet, attraverso materiali resi disponibili sui canali di comunicazione usati dalla scuola.

Per gli studenti:

- all'inizio dell'anno scolastico, in occasione dell'illustrazione del regolamento di Istituto agli alunni, verrà presentata questa policy;

- nel corso dell'anno ciascun docente dedicherà alcune lezioni alle buone pratiche per un utilizzo sicuro del digitale, con specifico riferimento ai rischi della rete e alla lotta al cyberbullismo.

Per i genitori:

- la proposta di incontri di sensibilizzazione, sul tema della sicurezza informatica, e di informazione circa i comportamenti da monitorare o da evitare.

1.4 ***Gestione delle infrazioni alla Policy***

Compito della Scuola è 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. Tale principio è alla base dello Statuto delle studentesse e degli studenti, nel quale si evidenzia la finalità educativa dei provvedimenti disciplinari, tesi a ripristinare comportamenti corretti all'interno dell'istituto "attraverso attività di natura sociale e culturale e in generale a vantaggio della comunità scolastica".
(Linee di orientamento per la prevenzione e il contrasto del cyberbullismo, ottobre 2017).

Le infrazioni alla policy possono essere rilevate da docenti/ATA nell'esercizio delle proprie funzioni oppure possono essere segnalate da alunni e genitori a docenti/ATA. Qualora essi si configurino come vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente scolastico per gli adempimenti del caso.
É bene ricordare che, nel momento in cui qualunque attore della comunità scolastica venga a conoscenza di un reato perseguibile d'ufficio, è fatto obbligo di denuncia (ex art. 331 del Codice di procedura penale). L'omissione di denuncia costituisce reato (art. 361). Tra i reati, che in ambiente scolastico sono riferiti all'ambito digitale e sono commessi per via telematica, si segnalano:

- Minaccia e, in particolare se la minaccia è grave, per tale reato si procede d'ufficio (art. 612 Codice penale)
- Induzione alla prostituzione minorile (art. 600 bis)
- Pedopornografia (art. 600 ter)
- Corruzione di minorenne (art. 609 quinquies).

Nel caso in cui le infrazioni della e-policy violino le norme previste dal Regolamento di Istituto, si rimanda al documento stesso. Le infrazioni verranno gestite in relazione alla loro gravità e, nel caso degli alunni, anche rispetto alla loro età. Per i provvedimenti disciplinari da adottare da parte del consiglio di classe nei confronti dell'alunno che ha commesso un'infrazione alla policy si rimanda al regolamento di disciplina dell'istituto.

<u>Infrazioni del personale scolastico</u>

- ✓ Le infrazioni alla policy da parte del personale scolastico possono riguardare sia la mancata osservanza delle regole sulla gestione della strumentazione, sia la mancata sorveglianza e il pronto intervento in caso di infrazione da parte degli alunni. Nel primo caso si valuterà la gravità derivata dall'esposizione al rischio procurata agli alunni, nel secondo caso si terrà in considerazione il danno procurato per la non tempestiva attivazione delle azioni enunciate. In quest'ambito la gestione delle infrazioni ricade nella disciplina contrattuale.

1.5 ***Monitoraggio dell'implementazione della Policy e suo aggiornamento***
Il monitoraggio per l'implementazione della Policy potrà avvenire al termine dell'anno scolastico, contestualmente all'aggiornamento del Rapporto di Autovalutazione e sulla base dei casi problematici riscontrati e della loro gestione, oppure all'inizio dell'anno scolastico, in fase di revisione del PTOF; attraverso la somministrazione ad alunni e docenti di questionari, si potrà verificare l'insorgenza di nuove necessità e/o la revisione delle tecnologie esistenti.

1.6 ***Integrazione della Policy con i Regolamenti esistenti***
La Policy è coerente con quanto stabilito dalla Legge (Statuto degli studenti e delle studentesse della scuola secondaria; Legge 29 maggio 2017 n. 71 "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyber bullismo"; Legge 31 dicembre 1996 n. 675 "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali"), dai Regolamenti vigenti (di Istituto, interno degli alunni) e dal Patto di Corresponsabilità.

2. Gestione dell'infrastruttura e della strumentazione TIC della scuola

2.1 ***Accesso a internet: filtri, antivirus e navigazione***
L'accesso a internet è possibile nella scuola primaria e nella scuola secondaria in tutte le aule, dotate di LIM con relativo computer. Le manutenzioni sono affidate al tecnico comunale e, in parte, al referente TIC d'Istituto, mentre è in carico a ciascun docente la segnalazione di malfunzionamenti e disservizi. I docenti hanno piena autonomia nel collegamento ai siti web nelle postazioni a loro riservate.

2.2 ***Gestione accessi (password, backup, ecc.)***
I computer presenti nelle aule richiedono una password di accesso per l'accensione. Ogni docente è tenuto al controllo della strumentazione in aula poiché l'uso del dispositivo è permesso agli alunni solo su autorizzazione dell'insegnante. Ogni docente accede al registro elettronico attraverso una password personale che non può essere comunicata a terzi.

2.3 ***Sito web della scuola***
Il sito dell'Istituto Comprensivo è http://www.icappianogentile.gov.it/
Il sito prevede un'area pubblica per le comunicazioni, che non riguardano la diffusione di dati personali o riservati, in cui sono reperibili le informazioni sulla vita scolastica, iniziative e scadenze ministeriali, avvisi di carattere generale e un'area riservata accessibile solo dopo autenticazione.
Il personale, che è in possesso delle credenziali per la gestione dei contenuti sul portale, si assumerà la responsabilità di garantire che il contenuto inserito sia accurato e appropriato.
.
2.4 ***Protezione dei dati personali***
In merito alla protezione dei dati personali, si fa riferimento a quanto previsto dal Decreto legislativo DECRETO LEGISLATIVO 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)" , nonché alla recente guida "La scuola a prova di privacy", a cura del Garante per la Protezione dei Dati personali). Il personale scolastico si impegna a trattare i dati personali nei limiti di legge quando necessarie ai fini dello svolgimento della propria funzione. Tutto il personale riceve istruzioni relative al trattamento dati personali ai fini della protezione e sicurezza degli stessi.
In caso di attività di ampliamento dell'offerta formativa, organizzate in collaborazione con Enti esterni, viene richiesto preventivamente ai genitori il consenso informato alle riprese audio/video e al loro eventuale utilizzo per scopi didattici, informativi e divulgativi anche tramite pubblicazione sul sito web. L'accesso ai dati riportati nel registro elettronico (ritardi, assenze, note e valutazioni) è riservato ai genitori tramite la consegna di una password di accesso strettamente personale.

3. Strumentazione personale

3.1 ***Strumentazione personale nella comunità scolastica***
Gli alunni non possono utilizzare i propri dispositivi durante le attività didattiche, se non autorizzati dai docenti; possono accedere alla rete solo su autorizzazione dell'insegnante presente in aula ed esclusivamente per finalità attinenti alle attività didattiche. Gli insegnanti possono utilizzare in classe i dispositivi della scuola, per realizzare tutte le attività connesse alla funzione docente e all'attività didattica.

4. Prevenzione, rilevazione e gestione dei casi

4.1 ***Prevenzione***
Gli operatori delle scuola, in modo particolare gli insegnanti, sono promotori e garanti della costruzione dialogica di un percorso formativo partecipato, e nel loro ruolo diventano confidenti degli alunni. Proprio per questo i docenti sono spesso i primi a rilevare le problematiche e i rischi che bambini e adolescenti possono trovarsi ad affrontare ogni giorno. Si pensi ai numerosi casi di bullismo e di cyberbullismo di cui gli insegnanti vengono a conoscenza e che si trovano ad affrontare durante l'anno scolastico. E' compito degli insegnanti imparare a riconoscere i rischi più comuni che i ragazzi possono correre sul web, per poter poi intervenire adeguatamente. Un'attenzione specifica andrà prestata ai fenomeni di bullismo/cyberbullismo, di sexting e di adescamento.

4.2 ***Rilevazione***
La rilevazione dei casi è compito dell'intera comunità educante, secondo la sensibilità di ciascuno e la presenza in particolari momenti o contesti. Il personale scolastico, soprattutto nella componente docente, ma anche in quella del personale ATA, è invitato a evitare atteggiamenti accusatori o intimidatori, in modo tale da riuscire a ricevere dai minori più fragili segnalazioni e confidenze circa situazioni problematiche vissute. É fondamentale osservare per tempo ciò che accade, per poter agire immediatamente e scongiurare conseguenze a lungo termine ben più gravi e negative per il benessere e la crescita armonica dei minori coinvolti.

Qualora si riscontri la pubblicazione di:

- dati sensibili o riservati (foto, immagini, video personali, informazioni private proprie o di amici, l'indirizzo di casa o il telefono, ecc.);
- contenuti che possono considerarsi in qualche modo lesivi dell'immagine altrui (commenti offensivi, minacce, osservazioni diffamatorie o discriminatorie, foto o video denigratori, videogiochi che contengano un'istigazione alla violenza, ecc.);
- contenuti riconducibili alla sfera sessuale: messaggi, immagini o video a sfondo sessuale, come foto di nudo o semi-nudo, ecc.

occorrerà prontamente segnalarli per gli interventi opportuni.

Il personale della scuola, anche con l'ausilio del tecnico di laboratorio, dell'Animatore digitale, del referente TIC d'Istituto provvederà a osservare le eventuali tracce di una navigazione non consentita su internet o del passaggio di materiali inidonei sui pc della scuola nonché la data e l'ora. Nel caso di messaggi, si cercherà di risalire al mittente attraverso i dati del suo profilo. In caso di abuso, l'insegnante dovrà copiare e stampare i messaggi per fornire le eventuali prove all'indagine sugli abusi commessi e raccogliere testimonianze sui fatti da riferire al Dirigente scolastico, alla famiglia ed, eventualmente, alla Polizia Postale. Qualora siano coinvolti più alunni, in qualità di vittime o di responsabili della condotta scorretta, le famiglie degli alunni in questione saranno convocate e informate tempestivamente per un confronto.

4.3 ***Gestione dei casi***

<u>Definizione delle azioni da intraprendere a seconda della specifica del caso</u>
La gestione dei casi rilevati va differenziata a seconda della loro gravità e, tuttavia, è opportuno condividere ogni episodio a livello di Consiglio di classe/team docenti. Alcuni avvenimenti possono essere affrontati e risolti con la discussione collettiva in classe. In altri è opportuno convocare genitori e alunni per cercare di rimediare all'accaduto. Nei casi più gravi occorre sottoporre all'attenzione del Dirigente scolastico l'accaduto perché predisponga le azioni da intraprendere.
È opportuno:

- Promuovere campagne di sensibilizzazione e informazione, con attività durante le ore curricolari e/o con l'ausilio di esperti o stimoli esterni (interventi di polizia postale, visione di film e spettacoli sul tema, seguiti da una adegata discussione);
- Portare a conoscenza degli alunni dei rischi di una eccessiva esposizione su internet, che può renderli implicati in episodi di cyberbullismo come responsabili o vittime; che per la legge italiana il cyber bullismo, la diffusione e il possesso di materiale pornografico è reato e che una foto o un video diffuso in rete potrebbero non essere tolti mai più.
- Sensibilizzare la popolazione studentesca sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni e per indurli alla prostituzione.
- Coinvolgere i genitori per attivare forme di controllo della navigazione e monitorare l'esperienza online dei propri figli.
- Tutelare la privacy e informare sull'esistenza di leggi in materia di tutela dei dati personali e di organismi per farle rispettare.
- Trattare, in classe, il bullismo, l'adescamento, l'uso sicuro di internet e dei social network, il sexting, il cyberbullismo e le loro conseguenze. Proporre riflessioni sulle menzogne dette per stringere relazioni online.
- Segnalare agli alunni l'esistenza:
- - di una linea di ascolto 19696 attiva tutto l'anno 24 ore su 24 per accogliere richieste di aiuto e di ascolto;
  - di un'app "You Pol", che permette di inviare in tempo reale alle sale operative della Polizia di Stato immagini, video, link, segnalazioni scritte allo scopo di denunciare episodi di bullismo e di cyber bullismo.
- Dotare i dispositivi della scuola di filtri che impediscano l'accesso a siti web non adatti ai minori (black list).

Per un'efficace gestione dei casi la scuola ritiene di dover tener traccia di ciò che è avvenuto rispetto ai comportamenti online scorretti da parte degli studenti e alla gestione del problema.

Il presente documento è approvato con delibera del Collegio dei Docenti e dal Consiglio d'Istituto.