ISTITUTO COMPRENSIVO STATALE
DI CAMPOLONGO MAGGIORE E CAMPAGNA LUPIA
Via ROMA, 47 30010 Campolongo Maggiore (VE)
Tel: 0495848146 - Fax: 0499744126
Cod. Mecc.: VEIC80800A - C.F.: 82011520275 – CUF: UF5AM0
e-mail: veic80800a@istruzione.it - P.E.C.: veic80800a@pec.istruzione.it

E- SAFETY POLICY

A.S 2018/2019

(ALLEGATO N 9)



Indice

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 Regolamenti esistenti.

2. Formazione e Curricolo

2.1 Curricolo sulle competenze digitali per gli studenti.

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

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

2.4 Sensibilizzazione delle famiglie.

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

3.1 Accesso ad internet: filtri, antivirus e sulla navigazione.

3.2 Gestione accessi

3.3 Sito web della scuola

3.4 Protezione dei dati personali

4. Strumentazione personale

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

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

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

5. Prevenzione, rilevazione e gestione dei casi

5.1 Prevenzione

5.1.1 Rischi

5.1.2 Azioni

5.2 Rilevazione

5.2.1 Che cosa segnalare

5.2.2 Come segnalare: quali strumenti e a chi.

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

1. Introduzione

1.1 Scopo della Policy

Il documento intende fornire le linee guida che l'Istituto Comprensivo "Aldo Moro" ha stabilito in materia di utilizzo consapevole delle TIC e di prevenzione/gestione di situazioni problematiche relative all'uso delle tecnologie digitali.

La partecipazione al progetto GENERAZIONI CONNESSE, promosso dal MIUR in collaborazione con la Comunità Europea, ha portato la nostra scuola a riflettere sui documenti recenti emanati dal Miur (LINEE GUIDA 2015 e PNSD) e a partire da questi per costruire delle solide basi per un futuro di consapevolezza e azione.

1.2 Ruoli e Responsabilità

Nell'ambito di questa policy sono individuati i seguenti ruoli e le principali responsabilità correlate:

Dirigente scolastico:

Deve garantire la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri della comunità scolastica; ha il compito di predisporre per propri docenti una formazione di base sulle Tecnologie dell'Informazione e della Comunicazione (ICT) che consenta loro di possedere le competenze necessarie all'utilizzo di tali risorse; monitora e controlla la sicurezza della rete interna all'istituto.

Docenti:

Devono provvedere personalmente alla propria formazione e al proprio aggiornamento sull'utilizzo del digitale curando l'approfondimento di tematiche legate alla dimensione etica e alla lotta al cyberbullismo. Fondamentale diventa la capacità di instillare negli alunni la consapevolezza dei rischi e dell'utilità della rete così da permetterne un uso corretto sia nel contesto scolastico che extrascolastico. Questo ovviamente dopo aver provveduto allo sviluppo delle competenze digitali. È dovere dei docenti segnalare prontamente alle famiglie eventuali problematiche riscontrate in classe o comunque nel contesto scolastico e informare il Dirigente scolastico e i suoi collaboratori sugli episodi di violazione delle norme di comportamento stabilite dalla scuola, prendendo i giusti provvedimenti.

***Animatore digitale*:**

Questa figura, di recente introduzione nel contesto scolastico, riveste particolare importanza nella corretta attuazione della policy. Ha il dovere di curare la propria formazione continua e di provvedere alla formazione interna alla scuola prevedendo attività laboratoriali e interattive. Deve essere in grado di trovare metodologie e strumenti innovativi che permettano la crescita e lacondivisione della cultura digitale. Deve, infine, mettere in pratica e sviluppare i dettami del Piano Nazionale Scuola Digitale.

Direttore dei Servizi Generali e Amministrativi:

Ha il compito di assicurare, nei limiti delle risorse finanziarie 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; deve curare la registrazione dei disservizi e delle problematiche relative alla rete e all'uso del digitale segnalate dai docenti, provvedendo all'intervento del personale tecnico di assistenza.

Studenti:

Devono essere in grado di mettere in pratica le indicazioni e le regole fornite dai docenti così come stabilite nella e-safety policy. Devono tutelarsi e tutelare i compagni da situazioni di rischio essendo consapevoli della necessità di richiedere l'aiuto di insegnanti e genitori. Devono infine curare l'approfondimento delle conoscenze digitali per arrivare a possedere solide competenze digitali.

Genitori:

La collaborazione e la sinergia con il contesto scolastico è fondamentale. È necessario che i genitori seguano con attenzione il percorso di sensibilizzazione e conoscenza in merito alla sicurezza in rete. Devono incoraggiare l'impiego delle TIC e segnalare eventuali situazioni problematiche riscontrate.

1.3 Condivisione e comunicazione della Policy all'intera comunità scolastica

La pregnanza di questo documento deve servire da stimolo per promuovere e attuare future azioni e iniziative. La e-safety policy rappresenta, infatti, il terreno fertile su cui costruire una solida rete fatta di scambio e collaborazione tra i diversi attori coinvolti.

Il **personale scolastico** riceverà, attraverso la pubblicazione in Drive, del materiale formativo sull'uso di Internet e le buone pratiche per prevenire e contrastare il cyberbullismo. Inoltre sarà informato, mediante la presentazione completa del documento, durante il collegio docenti, sotto la supervisione del Dirigente scolastico. Questo dopo discussioni e riflessioni precedenti tenute nei consigli di classe e nei dipartimenti disciplinari. La referente scolastica al progetto resterà a disposizione dei colleghi e li seguirà nella progettazione e messa in pratica di attività e laboratori di classe.

Agli **studenti** verrà illustrata la policy all'inizio dell'anno scolastico. In questa occasione si farà menzione, inoltre, del regolamento interno di istituto e di tutti i documenti ad esso collegati. Sarà inoltre presente uno sportello d'ascolto dedicato ad eventuali dubbi e necessità gestito dal referente al cyberbullismo e dall'animatore digitale.

I **genitori** saranno informati mediante incontri di formazione e confronto e attraverso la condivisione di materiale informativo.

1.4 Gestione delle infrazioni alla Policy

La gestione delle infrazioni seguirà criteri diversi in base alla persona coinvolta, alla sua età e al grado di gravità dell'azione compiuta.

Infrazioni del personale scolastico

La disciplina contrattuale e la base da cui valutare le infrazioni del personale educativo. In particolare saranno valutati due aspetti: la vigilanza deficitaria e l'incapacità di intervenire attivamente nei casi di infrazione degli alunni. Questi due casi, infatti, implicano sia l'incapacità di mettere in pratica le azioni concordate in questo documento sia la sottovalutazione dei rischi per gli studenti coinvolti.

Infrazioni degli alunni

Le infrazioni sono eventi da prevenire quanto più è possibile. A questo scopo appare necessario attivare situazioni di riflessione, condivisione e laboratori che instillino il seme della consapevolezza legata agli effetti dell'uso improprio della rete. Il consiglio di classe, tenendo conto dei criteri sopra citati, agirà dapprima con un richiamo verbale e un avviso ai genitori sul diario personale e, in seguito, con assegnazione di attività aggiuntive su tematiche di Cittadinanza e Costituzione. Qualora la gravità lo richiedesse verranno predisposti colloqui tra genitori e insegnanti e genitori e Dirigente scolastico.

Infrazioni dei genitori

La collaborazione tra scuola e famiglia è alla base della costruzione di un percorso valido per mettere in atto azioni di supporto e contrasto dei rischi legati alla rete. Qualora i genitori fossero protagonisti di comportamenti non educativi e che prevedano un danno ai minori, sono previsti interventi, in base alla gravità, che vanno dalla semplice comunicazione scritta o telefonica fino alla convocazione da parte degli insegnanti e/o del Dirigente scolastico.

1.5 Monitoraggio dell'implementazione della Policy e suo aggiornamento

Il monitoraggio dell'implementazione della Policy avrà luogo al termine di ogni anno scolastico, in collegamento alla raccolta di dati utili riguardanti le infrazioni, i casi registrati e la loro gestione e contestualmente al Rapporto di Autovalutazione. L'aggiornamento avverrà, invece, all'inizio di ogni anno scolastico, contestualmente alla revisione del PTOF, a cura del Dirigente scolastico, dell'Animatore digitale e dei collaboratori del Dirigente, per verificare la necessità di eventuali revisioni tecniche e non.

1.6 Integrazione della Policy con Regolamenti esistenti

Il documento si lega strettamente al regolamento interno d'istituto e al PTOF. Inoltre si collega ad una serie di buone pratiche riguardanti l'utilizzo di internet, dei computer e del laboratorio di informatica.

In particolare va ricordato che:

- I software installati e le apparecchiature sono ad esclusivo uso didattico e devono essere conformi alle leggi sul copyright;
- I computer e le apparecchiature dentro la scuola costituiscono un patrimonio comune, per questo vanno trattati con cura e rispetto e non sono ammesse manomissioni e alterazioni;
- l'ingresso degli studenti nel laboratorio di informatica avviene solo in presenza di un docente;
- i docenti devono accertarsi di non lasciare incustodite le apparecchiature e il laboratorio e devono accertarsi che, una volta concluse le attività, l'ambiente sia ordinato e non ci siano macchine accese;
- cd e chiavette usb devono sempre essere controllati prima del loro utilizzo e il loro inserimento e la loro estrazione deve avvenire secondo le pratiche apprese (espulsione sicura ecc.);
- in caso di malfunzionamenti o riscontro di alterazioni bisogna subito darne segnalazione;

- il Responsabile di laboratorio comunicherà tempestivamente al Dirigente Scolastico le eventuali violazioni avvenute e avrà cura di tenere un calendario aggiornato dell'utilizzo del laboratorio da parte di classi e insegnanti.

2. Formazione e Curricolo

2.1 Curricolo sulle competenze digitali per gli studenti

Le nuove tecnologie sono diventate una realtà quotidiana. Il mondo della scuola deve quindi mostrarsi pronto e ricettivo nell'assumere il ruolo di tramite non solo per la mera conoscenza delle TIC e di Internet, ma anche per la costruzione di competenze solide che rendano in grado gli studenti di entrare nell'universo digitale avendone cura e padronanza. Per questo l'uso delle risorse digitali deve stringersi a doppio filo con il curricolo disciplinare e interdisciplinare. Solo così si potrà dare vita ad una vera cittadinanza digitale. Appare chiaro che ad ogni grado di istruzione corrisponderanno competenze diverse che si differenziano soprattutto in relazione ai concetti di consapevolezza e responsabilità.

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

Per il personale docente saranno predisposti degli appositi corsi di formazione sulle competenze digitali. Nella pratica quotidiana lo scambio di conoscenze tra docenti già formati (es. animatore digitale, docente responsabile delle risorse informatiche) e non, permette la crescita della consapevolezza e una maggior destrezza nella pratica di utilizzo. Inoltre vengono resi disponibili numerosi materiali che consentono l'avanzamento dell'autoformazione e/o lo stimolo per la condivisione assieme agli studenti.

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

La formazione specifica dei docenti sull'utilizzo consapevole e sicuro di Internet, prevede 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. Il sito della scuola dedica uno spazio alla presentazione di alcuni programmi che possono essere utilizzati nella pratica didattica. L'animatore digitale coadiuvato da altri docenti ha inoltre condiviso in Drive materiali funzionali alla pratica del digitale.

2.4 Sensibilizzazione delle famiglie

Il nostro istituto ha sempre prestato grande attenzione e cura nell'organizzazione di momenti di sensibilizzazione e scambio dedicati a genitori, docenti e alunni. Quest'anno gli studenti delle prime e seconde classi della scuola secondaria sono state coinvolte nel progetto "Cyber me", riguardante il rapporto tra digitale ed empatia. Le classi seconde sono coinvolte, inoltre, nel progetto promosso dall'asl locale "Non cadere nella rete". Le famiglie sono state rese partecipi degli obiettivi e delle azioni legati a queste iniziative e si sono dimostrati entusiasti. Ogni anno l'istituto organizza all'interno del Centro civico comunale degli incontri con esperti, dedicati ai genitori, sull'uso delle tecnologie. Sarà cura della scuola diffondere informazioni e materiali di "Generazioni Connesse" e rendere visibile sul sito questo documento.

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

3.1 Accesso ad internet: filtri, antivirus e sulla navigazione

Una navigazione totalmente sicura è impossibile da garantire ma la scuola metterà in campo tutte le sue risorse e attuerà tutte le azioni possibili per creare un ambiente didattico senza rischi. L'accesso a internet è possibile, nella scuola primaria e nella scuola secondaria, nelle aule dotate di LIM e computer fisso e nel laboratorio di informatica. Le impostazioni sono definite dal responsabile dei laboratori e dall'Animatore digitale ed 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. Gli alunni che hanno accesso a Internet durante l'attività didattica saranno guidati nella navigazione dall'insegnante e potranno lavorare alla stesura di documenti collaborativi purché sotto il controllo del docente.

3.2 Gestione accessi (password, backup, ecc.)

I computer presenti in aula insegnanti prevedono una password di accesso, comunicata ai docenti all'inizio dell'anno scolastico, mentre i pc nelle aule non richiedono una password d'accesso. Sarà quindi cura dei docenti valutare eventuali alterazioni o file sospetti, oltre che un utilizzo consono e autorizzata da parte degli studenti. Il registro elettronico prevede una password personale da non comunicare a terzi mentre l'accesso al Drive d'istituto prevede una gmail assegnata dall'animatore digitale e una password cambiata dal docente dopo il primo accesso, anch'essa da tenere segreta.

3.3 Sito web della scuola

Il sito dell'Istituto Comprensivo è http://www.aldomorocampagnalupia.gov.it/. Il sito è strutturato in modo tale che siano presenti un'area pubblica fruibile dal pubblico per reperire informazioni sull'istituto ed essere aggiornati sulle attività, i progetti e gli avvisi generali, e un'area riservata a cui Il personale amministrativo e scolastico può accedere solo mediante l'inserimento di una apposita password. La responsabilità del mantenimento delle informazioni è chiaramente a cura del personale.

3.4 Social Network

La nostra scuola non ha profili social in rete. Gli studenti sono invitati a non diffondere illecitamente foto, video e registrazioni senza previa autorizzazione. Genitori e allievi sono invitati ad un utilizzo conscio dei Social Network, in particolare Facebook e Whatsapp, strumenti che spesso si utilizzano senza una piena assunzione di responsabilità.

3.5 Protezione dei dati personali

Il personale incaricato riceve una formazione riguardante le pratiche di trattamento dei dati personali e della privacy. Per progetti e attività che richiedono foto e/o riprese viene utilizzato il modello di liberatoria presentato da "Generazioni connesse", che deve essere compilato e firmato. 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.

4. Strumentazione personale

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

Come prevede il regolamento d'istituto non è consentito agli studenti l'uso di strumenti elettronici personali né quello del cellulare. L'eventuale uso di computer e tablet è permesso solo su previa autorizzazione del docente e solo a scopi didattici. Nella scuola primaria si chiede alle famiglie di non lasciare tali dispositivi ad alunne e alunni; nella scuola secondaria di primo grado all'ingresso in aula, i dispositivi devono essere spenti. Nel caso in cui gli studenti debbano comunicare con la famiglia durante l'orario scolastico, possono usare gratuitamente la linea fissa della scuola rivolgendosi a un operatore; allo stesso modo le famiglie devono chiamare il centralino della scuola se hanno assoluta necessità di parlare con i propri figli. Tali comunicazioni saranno ridotte a casi di inderogabile necessità e urgenza. Gli alunni con disturbi specifici di apprendimento concorderanno le modalità di impiego di strumenti compensativi quali tablet e computer portatili.

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

Il personale docente ha la possibilità di usare le apparecchiature digitali proprie e della scuola a scopi didattici. L'uso personale non è invece consentito e il cellulare è previsto solo in caso di chiamate e comunicazioni urgenti.

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

Al restante personale di servizio l'uso del cellulare è permesso solo per comunicazioni di carattere urgente mentre è vietato l'uso di altre apparecchiature proprie.

5. Prevenzione, rilevazione e gestione dei casi

5.1 Prevenzione

5.1.1 Rischi

Gli insegnanti rivestono un ruolo complesso che prevede non solo un aspetto educativo, ma soprattutto umano. Il dialogo e lo scambio emotivo con i propri studenti è uno dei motori propulsivi per garantire un percorso formativo di qualità. Per questo i docenti sono una sorta di vedetta, un faro sicuro nel mare in tempesta in grado di salvare i marinai in pericolo. La sensibilità e le competenze del corpo docente consentono di individuare le situazioni di rischio, riconoscerne il grado di gravità ed intervenire in maniera adeguata

5.1.2 Azioni

Dopo aver verificato una situazione di pericolo risulta essenziale agire in tempi brevi e in modo mirato per minimizzare le conseguenze ed evitare ulteriori danni.

Per agevolare ciò sono necessari i seguenti interventi:

- rendere la diffusione delle informazioni e dei materiali di "Generazioni Connesse" capillare all'interno della comunità scolastica;
- dotare la scuola di dispositivi atti al filtraggio e al contrasto di tentativi di violazione e uso scorretto dei dispositivi;
- rigido controllo sui siti utilizzati dagli studenti e sul loro attenersi ai divieti (es. utilizzo cellulari i orario scolastico.

5.2 Rilevazione

5.2.1Che cosa segnalare

Sono da segnalare tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona (o un piccolo gruppo) tramite un utilizzo irresponsabile dei social network. In particolare si segnaleranno:

- contenuti afferenti la violazione della privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, ecc.);
- contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.);
- contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), ecc

Sarà compito dei docenti registrare le segnalazione negli appositi documenti (vedi allegati).

5.2.2 Come segnalare: quali strumenti e a chi.

La segnalazione è il primo passo per arrivare alla risoluzione di situazioni sgradevoli e che mettono gli studenti in una situazione di pericolo. Gli insegnanti, coadiuvati dal tecnico della scuola e dall'Animatore digitale, devono raccogliere prove valide delle condotte errate. Questo sarà possibile soprattutto quando il comportamento errato abbia avuto come mezzo i pc della scuola. Qualora gli abusi siano legati al telefono cellulare sarà necessario che eventuali messaggi rimangano salvati nel dispositivo così da poter far conoscere i fatti a genitori e Dirigente e, nei casi più seri, alle forze di Polizia. Quando l'unica fonte è rappresentata dalle testimonianze dell'alunno, le notizie raccolte sono comunque comunicate ai genitori e per fatti rilevanti anche al Dirigente scolastico. In particolare la segnalazione viene fatta a entrambe le famiglie, se oltre alla vittima anche l'autore della condotta negativa è un altro alunno.

Le segnalazioni prevedono il seguente iter, declinabile in base alla gravità dell'accaduto:

- annotazione del comportamento sul registro e comunicazione scritta ai genitori;
- convocazione scritta e colloquio con i genitori degli alunni, da parte dei docenti;
- relazione scritta al Dirigente scolastico.

Qualora la situazione risultasse grave, l'obbligo sarà quello di avvisare le autorità giudiziarie ed, eventualmente, ricorrere ai servizi messi a disposizione dal Safer Internet Center.

5.3 Gestione dei casi

La gestione dei casi e quindi le buone pratiche di prevenzione, segnalazione e azione, seguono i protocolli resi disponibili da "Generazioni Connesse". A seguire sono proposti gli allegati con gli schemi guida.

La Referente del Progetto — Il Dirigente Scolastico

Prof.ssa Serena Faggian — Dott.ssa Fulvia Salmaso

Campagna Lupia, giugno 2018

Schema riepilogativo delle situazioni gestite legate a rischi online (ALLEGATO N.2)

Riepilogo casi

Scuola_____ Anno Scolastico_____

N°	Data	ora	Episodio *(riassunto)*	Azioni intraprese		Insegnante con cui l'alunno/a si è confidato	Firma
				Cosa?	Da chi?		

Sicurezza in rete - Schema per la scuola

Cosa fare in caso di... cyberbullismo?

Alunno/a preso in giro/minacciato/offeso online

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**

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

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**