MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA
ISTITUTO COMPRENSIVO STATALE "A. FRANK"
Via Boccaccio, 336 20099 - Sesto San Giovanni ☏ 02-2481175 02-24411406
www.icsfrank-sestosg.gov.it email: miic8a100t@istruzione.it pec: miic8a100t@pec.istruzione.it
C. F. 94581330159 C/C Postale n° 21371265 Codice fatturazione UF47TH

DOCUMENTO

di *E-SAFETY POLICY*

anno scolastico 2018/19

INDICE:

Il presente documento viene elaborato seguendo le indicazioni delle Linee di Orientamento per azioni di Prevenzione e di contrasto al bullismo e cyberbullismo (aprile 2015 e aggiornamenti ottobre 2017) elaborate dal Ministero dell'Istruzione, dell'Università e della Ricerca in collaborazione con Generazioni Connesse e il Safer Internet Center per l'Italia.

1. INTRODUZIONE:

Data la pervasività delle tecnologie nella quotidianità e la notevole familiarità degli alunni con gli strumenti informatici, la scuola è chiamata non solo a redigere un codice di comportamento al quale tutti i membri della comunità scolastica sono chiamati ad attenersi, al fine di garantire un ambiente adeguato all'utenza e sicuro, ma anche ad attivare percorsi di formazione per promuovere un uso responsabile della rete.
La Policy di E-safety è un documento autoprodotto dalla scuola, volto a descrivere una nuova visione del fenomeno della rete, le norme comportamentali e le procedure per l'utilizzo delle TIC in ambiente scolastico, le misure per la prevenzione e quelle per la rilevazione e gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali.

1a. Scopo della Policy di E-safety

L'intento del nostro Istituto e più in generale della scuola è quello di promuovere fra gli alunni un uso consapevole e critico delle tecnologie digitali e di internet, di far acquisire loro non solo procedure e competenze "tecniche", ma anche corrette norme comportamentali, di prevenire o fronteggiare problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso, delle tecnologie digitali.
Al fine di perseguire i suddetti obiettivi, l'E-Safety delinea le seguenti strategie:

- avvio di percorsi di formazione per un uso consapevole delle TIC rivolti agli insegnanti nel corso dell'anno scolastico;
- coinvolgimento dei genitori come partner educativi nei percorsi di formazione;
- controllo del sistema informatico da parte dei responsabili (cronologia, cookies);
- installazione di firewall sull'accesso Internet;
- presenza di un docente o di un adulto responsabile durante l'utilizzo di Internet o di altre TIC;
- aggiornamento periodico del software antivirus e scansione delle macchine in caso di sospetta presenza di virus;
- utilizzo di penne USB, CD/DVD o altri dispositivi esterni personali, solo se autorizzati.

In questo contesto, il Dirigente Scolastico, l'Animatore Digitale, il Referente del cyberbullismo e i docenti hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di indicare regole di condotta chiare per un uso critico e consapevole di internet anche a casa, per prevenire il verificarsi di situazioni pericolose.

1. b Ruoli e responsabilità

Il personale dell'Istituto, i genitori e gli alunni si impegnano formalmente a seguire le leggi vigenti e a rispettare codesto documento. Si fa esplicito divieto di utilizzare file o software non autorizzati e/o privi di licenza su tutti gli strumenti e i materiali informatici. Chi utilizza Internet a scuola e in ambiente extrascolastico per lo svolgimento di attività di studio e ricerca, esplicitamente richieste dalla scuola, deve rispettare il seguente regolamento. Non va dimenticato che la fruizione di Internet è tutelata e sanzionata da Leggi dello Stato. Ferme restando le strategie sistematiche messe in atto dalla Scuola, ciascun utente connesso alla rete deve:

- rispettare il presente regolamento e la legislazione vigente;
- 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 cosiddetta netiquette (regole condivise che disciplinano il rapportarsi tra utenti della rete, siti, forum, mail e di qualsiasi altro tipo di comunicazione).

Di seguito vengono indicati i ruoli e gli incarichi dei diversi soggetti coinvolti.

DIRIGENTE SCOLASTICO

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

- garantisce la sicurezza (tra cui la sicurezza on-line) dei membri della comunità scolastica;
- garantisce che tutti gli insegnanti ricevano una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze, e un utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della comunicazione (TIC);
- garantisce l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line;
- predispone filtri di protezione per l'accesso ad internet ad ogni postazione per evitare la navigazione di siti inadeguati;
- comprende e segue le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola;
- coordina linee di intervento per la gestione e la presa in carico dei casi di abuso o altre problematiche associate all'utilizzo di internet e delle tecnologie digitali.

DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI

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

- assicura, 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;
- garantisce il funzionamento dei diversi canali di comunicazione (circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni.
- garantisce che il personale ATA (assistenti amministrativi e collaboratori scolastici) rispettino le regole di utilizzo della rete internet, dei PC e degli altri dispositivi elettronici

ANIMATORE DIGITALE E REFERENTI DI PLESSO

L'Animatore digitale e i docenti referenti di plesso hanno i seguenti compiti:

- stimolano la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e forniscono consulenza e informazioni al personale in relazione ai rischi on-line e alle misure di prevenzione e gestione degli stessi;
- monitorano e rilevano le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, nonché propongono la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;
- coinvolgono la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti la "scuola digitale".

DOCENTE RESPONSABILE DEL SERVIZIO INFORMATICO

Il Responsabile del servizio informatico:

- assicura che gli utenti possano accedere alla rete della scuola solo tramite password applicate
- cura la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti (istruzione e formazione);
- propone al Dirigente e mette in atto tutte le misure tecniche che si rendono necessarie per garantire il rispetto della e-Policy
- mantiene i contatti con i Tecnici esterni: azienda fornitrice del registro elettronico, azienda fornitrice della rete dati (TIM, Fastweb, etc), servizio tecnico del Comune, consulente tecnico della scuola, azienda fornitrice del dominio per il sito (Aruba)

DPO Data Protection Officer

Il data Protection Officer (di seguito DPO) è una figura introdotta dal Regolamento generale sulla protezione dei dati 2016/679 | GDPR, pubblicato sulla Gazzetta Ufficiale europea L. 119 il 4 maggio '16.

Il DPO, figura storicamente già presente in alcune legislazioni europee, è un professionista che deve avere un ruolo aziendale (sia esso soggetto interno o esterno) con competenze giuridiche, informatiche, di risk management e di analisi dei processi. La sua responsabilità principale è quella di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno di un'azienda (sia essa pubblica che privata), affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali.

Questo soggetto è già conosciuto nel mondo anglosassone con il termine di Chief Privacy Officer (CPO); Privacy Officer, Data Protection Officer o Data Security Officer.

L'art. 39 del Regolamento europeo sulla protezione dei dati personali elenca i principali compiti del DPO (Responsabile della protezione dei dati):

1. Il responsabile della protezione dei dati | DPO | è incaricato almeno dei seguenti compiti:

a) informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento o del Responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;

d) cooperare con l'autorità di controllo; e

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

REFERENTE CYBERBULLISMO

Il ruolo del Referente Cyberbullismo include i seguenti compiti:

- essere interfaccia con le forze di Polizia, con i servizi minorili dell'amministrazione della Giustizia, le associazioni e i centri di aggregazione

giovanile sul territorio, per il coordinamento delle iniziative di prevenzione e contrasto del cyberbullismo;
- coordina azioni di sensibilizzazione per la diffusione di una cultura sull'uso consapevole delle TIC;
- propone strumenti e azioni per la prevenzione di situazioni a rischio;
- prevede, in accordo col Dirigente, linee di intervento per la gestione e la presa in carico dei casi di abuso o altre problematiche associate all'utilizzo di internet e delle tecnologie digitali;
- riferisce al Dirigente Scolastico situazioni o problemi di particolare rilevanza su cui intervenire

I DOCENTI

Il docente nel libero esercizio della sua professionalità:

- illustra ai propri alunni le regole contenute nel presente documento;
- espone il regolamento riguardante l'utilizzo di internet, degli strumenti informatici e dei relativi software per prevenire e contrastare l'utilizzo scorretto delle TIC e di internet;
- spiega agli alunni/e i diritti inerenti il copyright;
- si informa e si aggiorna sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet;
- offre indicazioni sul corretto utilizzo della rete condividendo la netiquette e indicandone le regole;
- guida la navigazione di studentesse e studenti, nelle lezioni in cui l'uso di Internet è pianificato, verso siti controllati come idonei per il loro uso, onde evitare di incontrare materiali inadatti;
- propone agli alunni attività di ricerca di informazione in rete fornendo opportunamente loro indirizzi dei siti e/o parole chiave per la ricerca cui fare riferimento;
- vigila che gli alunni non utilizzino le TIC senza l'autorizzazione e il controllo del docente, incorrendo in comportamenti illeciti;

Al docente è consentito l'utilizzo del portatile assegnato dall'Istituto, del pc presente nell'aula docenti, nei Laboratori di Informatica, nell'Aula LIM, solo se compatibile o funzionale al ruolo professionale svolto per:

1) la ricerca di informazioni o documenti
2) gli approfondimenti culturali/attualità
3) attività di studio e progettazione inerenti alla professione docente.

Tale utilizzo non deve essere causa diretta o indiretta di disservizi dei sistemi di collegamento e non deve generare oneri aggiuntivi per l'Amministrazione.

IL PERSONALE DOCENTE E ATA

- segnala prontamente eventuali malfunzionamenti o danneggiamenti al responsabile del servizio informatico ai fini della ricerca di soluzioni;
- segnala al Dirigente Scolastico e al Referente Scolastico del Bullismo e Cyberbullismo qualsiasi abuso rilevato a scuola, nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di internet;

- custodisce e non divulga le credenziali d'accesso degli account e delle reti Wi-fi;
- tratta i tutti i dati personali degli alunni, dei genitori e del personale scolastico nel rispetto della normativa vigente sulla privacy (Regolamento UE 679/2016);
- vigila sulla postazione e non l'abbandona se non prima di aver effettuato la disconnessione;
- lascia la postazione in ordine, sempre, sia nel laboratorio che in classe, avendo effettuato le corrette procedure per la disconnessione;
- non modifica nessuna impostazione data al monitor, al PC, alla LIM o agli altri supporti informatici e non salva sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili;
- non usa i pc della scuola per scopi privati, lasciando i propri account aperti o accessibili, ma solo per scopi didattici e per le finalità connesse con il ruolo e la funzione docente;
- non utilizza file o software non autorizzati e/o privi di licenza su tutti gli strumenti e i materiali informatici.
- si informa sulla sicurezza informatica, la politica dell'Istituto e relative buone pratiche;
- segnala qualsiasi abuso, anche sospetto, al Dirigente Scolastico o all'Animatore Digitale o al Referente Cyberbullismo per le opportune indagini / azioni / sanzioni.

STUDENTI

Gli **studenti** non sono solo destinatari, ma anche interlocutori privilegiati, attivi e propositivi di tutte le azioni e gli interventi volti alla piena attuazione della Policy.

Le alunne e gli alunni sono responsabili dell'utilizzo corretto dei sistemi informatici e della tecnologia digitale in accordo con i termini previsti da questa policy. In particolare:

- utilizzano le TIC su indicazioni del docente;
- sono responsabili, in relazione al proprio grado di maturità e di apprendimento, dell'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;
- conoscono e comprendono l'importanza delle buone pratiche di sicurezza online a tutela dell'incolumità propria e altrui;
- devono evitare il plagio e rispettare i diritti d'autore;
- devono essere informati sulle politiche d'uso dei dispositivi mobili e device digitali, sull'utilizzo delle immagini e sulla gestione della privacy;
- adottano condotte rispettose degli altri anche quando comunicano in rete;
- devono acquisire consapevolezza del significato e della gravità di atti di cyberbullismo;
- comprendono l'importanza della segnalazione di ogni abuso, uso improprio o accesso a materiali inappropriati;
- comunicano tempestivamente in caso di malfunzionamento e/o di contatto con informazioni immagini e/o applicazioni inappropriato;
- mantengono la configurazione del sistema operativo senza modificarlo;

- non utilizzano il proprio telefono cellulare e/o altri dispositivi elettronici e di intrattenimento (console portatili, mp3, ipod, ipad, notebook, fotocamera, videocamera) durante ogni attività scolastica;
- tengono i propri dispositivi spenti e opportunamente custoditi in zaini o altro luogo.

I GENITORI

Gli adulti hanno un ruolo fondamentale nel garantire che bambini/e ed adolescenti siano in grado di utilizzare le tecnologie digitali e che lo facciano in modo appropriato e sicuro, ruolo che vede coinvolti a pieno titolo tutti coloro che hanno un compito educativo, oltre che formativo, primi fra tutti i genitori e la comunità scolastica nel suo complesso.

L'impegno da parte dei genitori è quello di fissare delle regole da far rispettare, anche in ambito domestico, primariamente assistendo i minori nel momento dell'utilizzo della rete e ponendo in atto tutti i sistemi di sicurezza.

La scuola creerà occasioni per sensibilizzare i genitori attraverso incontri con esperti, circolari, sito web e altre comunicazioni telematiche, informazioni su campagne di sicurezza promosse da altre istituzioni o su convegni dedicati a questo tema.

I genitori saranno incoraggiati a sostenere la scuola nel promuovere le buone pratiche di E-safety.

Allo scopo di condividere regole comuni per l'utilizzo sicuro di Internet, sia a casa che a scuola, tutti i genitori sono tenuti a prestare la massima attenzione ai principi e alle regole contenute nel presente documento. In particolare:

- sostengono la linea di condotta della scuola adottata nei confronti dell'utilizzo delle TIC;
- conoscono le politiche di utilizzo delle immagini e la gestione della privacy;
- sono consapevoli del significato e della gravità di atti di cyberbullismo;
- accompagnano il figlio nella gestione di device (come lo smartphone);
- stabiliscono le regole e le modalità per il controllo delle attività svolte dai propri figli sulla rete per esempio installando parental control, limitando i tempi di accesso a internet e di uso dei videogiochi, etc
- verificano l'adeguatezza delle attività svolte dal ragazzo rispetto alla sua età e alla sua sensibilità;
- devono essere attenti ai comportamenti dei figli dopo la navigazione in internet o dopo l'uso prolungato del telefonino o del computer presente in casa.

1.c Condivisione e comunicazione della E-POlicy alla Comunità scolastica

La E-policy viene pubblicata sul sito della scuola nella sezione dedicata al cyberbullismo. A tutta la comunità scolastica si chiede di prenderne visione e condividerla. Per facilitare la presa in carico del documento si possono prevedere momenti di discussione collegiale sui contenuti, sulle pratiche indicate e su come inserire nel curricolo le tematiche di interesse della policy. Ogni modifica e miglioramento verrà opportunamente comunicata e condivisa.

Per la componente studentesca si potranno prevedere delle discussioni in classe sulla policy, sfruttando i primi giorni di scuola, con particolare riguardo al protocollo di accoglienza per le nuove classi prime. Per i genitori si potranno organizzare incontri di sensibilizzazione sul tema della sicurezza informatica e sui comportamenti da monitorare o da evitare.

1d. Gestione delle infrazioni alla E-Policy

La Legge 107 del 2015 ha introdotto, tra gli obiettivi formativi prioritari, lo sviluppo delle competenze digitali degli studenti, finalizzato anche a un utilizzo critico e consapevole dei social network e dei media, e declinato dal Piano Nazionale Scuola Digitale. 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. Tale principio è alla base dello Statuto delle studentesse e degli studenti che sottolinea la finalità educativa anche quando si rendano necessari provvedimenti disciplinari,comunque tesi a ripristinare comportamenti corretti all'interno dell'istituto "attraverso attività di natura sociale e culturale ed in generale a vantaggio della comunità scolastica." (*Linee di orientamento per la prevenzione e il contrasto del cyberbullismo – Ottobre 2017)*

Tutte le infrazioni alla presente Policy andranno tempestivamente segnalate al Dirigente Scolastico, che avrà cura di convocare le parti interessate onde valutare le possibili azioni da intraprendere.

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.

Qualora esse si configurino come vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso.

È bene ricordare che, nel momento in cui un 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).
DEVONO ESSERE DENUNCIATI i seguenti reati perseguibili d'ufficio:

- rapina ed estorsione (art 628 c.p e art 629 c.p.) riferibili a episodi di minacce e violenza per ottenere (sottrarre) oggetti o somme di denaro;
- lesioni gravissime (art. 582 c.p. – 585 c.p.) e lesioni guaribili in più di 40 giorni o che comportano una diminuzione permanente delle funzionalità di un organo;
- violenza sessuale – anche come cyberbullismo – (art. 609 c.p) commessa singolarmente o in gruppo – in questo caso viene considerata più grave e punita più severamente;
- violenza o minaccia a pubblico ufficiale per alunni che hanno compiuto il quattordicesimo anno di età (art. 336 c.p. e art. 337 c.p)

EPISODI DI BULLISMO PERSEGUIBILI in caso di querela:
lesioni lievi, minacce, ingiurie, diffamazione (art. 582, 612, 591. 595 c.p.). In questi casi è necessario informare la famiglia (o eventualmente segnalare il caso ai Servizi Sociali) che può procedere alla querela, a sua discrezione.

Nel caso in cui le infrazioni della e-policy violino norme previste dal Regolamento SEZIONE - Prevenzione e contrasto di "BULLISMO E CYBERBULLISMO" si procede secondo quanto previsto:

- http://www.icsfranksestosg.gov.it/attachments/article/148/REGOLAMENTOcyberbullismoFrank18.pdf

Potenziali infrazioni dei docenti
Il docente, nonché il personale scolastico (Dirigente, DSGA, Referente Cyberbullismo, Animatore digitale, assistente amministrativo), non deve pubblicare materiale scolastico sui siti o blog personali. La creazione di pagine online su social media relative a specifici progetti non deve contenere foto né dati sensibili che consentano di risalire alle generalità degli alunni.
"Non violano la privacy le riprese video e le fotografie raccolte dai genitori durante le recite, le gite e i saggi scolastici. Le immagini, in questi casi, sono raccolte per fini personali e destinate a un ambito familiare o amicale e non alla diffusione. Va però prestata particolare attenzione alla eventuale pubblicazione delle medesime immagini su Internet, e sui social network in particolare. In caso di comunicazione sistematica o diffusione diventa infatti necessario, di regola, ottenere il consenso informato delle persone presenti nelle fotografie e nei video" (Vademecum – *A scuola di privacy*) *https://www.garanteprivacy.it/documents/10160/0/Vademecum+ La+scuola+a+prova+di+privacy +pagina+singola+%28anno+2016%29.pdf*

Si sottolinea che ai docenti è fatto divieto di:

- utilizzare le tecnologie d'uso comune con gli alunni per attività non connesse all'insegnamento o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei;
- installare materiale protetto da copyright;
- collegarsi ad internet a scopi commerciali o di profitto personale e per attività illegali;
- trattare i dati personali comuni e/o sensibili degli alunni in modo non conforme ai principi della privacy;
- diffondere le password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- eludere la vigilanza degli alunni, favorendo un utilizzo non autorizzato delle TIC e possibili incidenti

Tutto il personale scolastico è tenuto a collaborare e a fornire ogni informazione utile per le valutazioni del caso e l'avvio dei procedimenti che possono avere carattere organizzativo, gestionale, disciplinare, amministrativo, penale, a seconda del tipo o della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.
Potenziali infrazioni delle studentesse e degli studenti
Alle studentesse e agli studenti è fatto divieto di:

- un uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare;
- l'invio incauto o senza permesso di foto o di altri dati personali;
- la condivisione di immagini intime o personali;
- il collegamento a siti web non indicati dai docenti;
- la comunicazione, incauta e senza permesso di un adulto, con sconosciuti su chat o blog;
- riprese o foto di compagni, docenti, o luoghi scolastici.

Se nonostante il divieto, gli alunni venissero sorpresi a usare il cellulare, lo stesso dovrà essere consegnato al docente e conservato in un luogo sicuro fino al termine dell'attività didattica.
Qualora eventuali fotografie o video effettuati illecitamente durante l'orario scolastico venissero ascritte all'ambito del reato, la scuola chiederà l'intervento degli organi competenti di Pubblica Sicurezza.

L'Istituzione Scolastica dopo aver messo in atto tutte le strategie per educare, prevenire, scoraggiare l'uso improprio del cellulare e altri dispositivi non previsti nell'ambito dell'attività scolastica, non si assume nessuna responsabilità, né relativamente all'uso improprio, né relativamente a smarrimenti o furti. Fermo restando che la scuola è un'istituzione educativa e che non è prevista, né possibile né legittima, la perquisizione quotidiana di tutti gli alunni/e, le responsabilità che dovessero derivare dal verificarsi di eventi riconducibili all'uso non legittimo di device non autorizzati sono totalmente ascrivibili alle famiglie degli alunni coinvolti.
Pertanto, in caso di infrazioni, si porranno in essere le sanzioni previste dal Regolamento di disciplina:

CONTRAVVENZIONI	**FREQUENZA**	**PROVVEDIMENTO**	**ORGANO COMPETENTE**
L'alunno ha il cellulare acceso (riceve chiamate o notifiche di messaggi)	Prima volta	Richiamo verbale e richiesta di spegnimento del cellulare	Docente

	Seconda volta	Richiesta di spegnimento del cellulare, nota sul registro di classe	Docente
	Uso reiterato	Richiesta di spegnimento e di consegna del cellulare, che sarà restituito solo al termine della giornata. Nota sul registro di classe. Convocazione della famiglia e richiesta di un C.d.C. straordinario per adozione provvedimenti disciplinari.	Coordinatore di classe, DS, Rappresentanti dei genitori
L'alunno utilizza dispositivi elettronici per chiamate o messaggi o per	Prima volta	Richiesta di spegnimento e di consegna del dispositivo che sarà	Docente

altro uso non consentito (giochi, musica, chat, etc.)		restituito solo al termine della giornata. Nota sul registro di classe, comunicazione alla famiglia.	
	Uso reiterato	Richiesta di spegnimento e di consegna del dispositivo, che sarà restituito solo al termine della giornata. Nota sul registro di classe. Convocazione della famiglia e di un C.d.C straordinario per adozione provvedimenti disciplinari.	Coordinatore di classe, DS, Rappresentanti dei genitori
L'alunno utilizza dispositivi elettronici durante una verifica scritta		Ritiro della verifica. Valutazione gravemente insufficiente. Nota sul registro di classe e	Insegnante

		comunicazione alla famiglia.	
L'alunno effettua riprese audio, foto e video		Richiesta di spegnimento e di consegna del dispositivo che sarà restituito solo al termine della giornata. Nota sul registro di classe e comunicazione alla famiglia. Convocazione del C.d.C per adozione provvedimenti disciplinari.	Coordinatore di classe, DS, Rappresentanti dei genitori
L'alunno diffonde a terzi, in modo non autorizzato, audio, foto, video in violazione alle norme sulla privacy		Richiesta di spegnimento e di consegna del dispositivo che sarà restituito solo al termine della giornata. Nota sul registro di classe con comunicazione alla	Coordinatore di classe, DS, Rappresentanti dei genitori

		famiglia. Convocazione del C.d.C per adozione provvedimenti disciplinari.	

2. FORMAZIONE CURRICOLO

2a. Curricolo sulle competenze digitali per la componente studentesca.

La Competenza digitale è ritenuta ormai una competenza. È evidente che le nuove tecnologie possono essere utilizzate al servizio di tutti i saperi e la "Competenza digitale" assume anch'essa dignità di linguaggio altamente trasversale.

Avere tali competenze per un alunno significa padroneggiare le abilità e le tecniche di utilizzo delle nuove tecnologie, ma soprattutto utilizzarle con "autonomia e responsabilità" nel rispetto degli altri e sapendone prevenire ed evitare i pericoli. Gli alunni dovrebbero quindi imparare ad utilizzare le TIC per cercare, esplorare, scambiare e presentare informazioni in modo responsabile, creativo e con senso critico, essere in grado di avere un rapido accesso a idee ed esperienze provenienti da persone, comunità e culture diverse. In questa ottica è stato strutturato il nostro curricolo digitale:

- promuovere un uso consapevole delle tecnologie;
- sensibilizzare e attivare gli studenti sui rischi e i pericoli derivanti da un uso non corretto dei social network;
- insegnare ciò che è lecito nell'utilizzo di Internet e ciò che è vietato, fornendo strumenti per l'utilizzo efficace di Internet e la conoscenza delle conseguenze delle violazioni;
- mostrare come produrre, pubblicare e presentare contenuti digitali in modo appropriato;
- insegnare la valutazione dei contenuti Internet;
- impiegare materiali prelevati da Internet a scopi didattici conformemente al diritto d'autore;
- favorire un approccio critico nelle alunne e alunni nella ricerca di materiali sul web, che permetta loro di vagliare la coerenza e la fondatezza delle informazioni trovate;
- insegnare le modalità di segnalazione di contenuti Internet sgradevoli o illegali.

2.b Formazione docenti sull'utilizzo e integrazione delle TIC nella didattica

Parte del corpo docente dell'Istituto A. Frank ha partecipato a corsi di formazione sull'uso delle TIC nella didattica organizzato dall'ambito territoriale 23 presso la l'Istituto copofila Montale di Cinisello B., sugli EAS (Episodi di Apprendimento Situato) a cura del CREMIT dell'Università Cattolica del Sacro Cuore di Milano ed infine al corso sul tema dell'uso consapevole della rete a cura del dott. Sergio Dicandia.
Il percorso di formazione specifica dei docenti sull'utilizzo delle TIC nella didattica, non si può ritenere esaurito, pertanto sono previsti, momenti di auto aggiornamento, di formazione personale o collettiva anche all'interno dell'istituto, con la condivisione delle conoscenze dei singoli e il supporto dell'Animatore digitale.

2c. Sensibilizzazione delle famiglie

In considerazione dell'importanza educativa della famiglia (vd. mission del PTOF d'Istituto), il presente documento completa Patto Educativo di Corresponsabilità stipulato con le famiglie degli alunni quale l'impegno reciproco di scuola e famiglia alla corresponsabilità formativa, nella quale rientrano a pieno titolo i temi legati alla e-Safety.

Allo scopo di mantenere viva l'attenzione delle famiglie su tali temi, l'Istituto promuove opportunità di incontro e formazione per le famiglie sui temi oggetto della Policy, offerte dal territorio, selezionando iniziative significative promosse da Enti e/o Associazioni di comprovata affidabilità. Nel corso dell'anno scolastico 2017/18, sono state promosse due iniziative aperte ai genitori degli alunni dell'I.C. Frank sull'uso consapevole della rete: una organizzata dagli esperti dagli esperti di Hewlett Packard Enterprise (http://www.icsfrank-sestosg.gov.it/index.php?option=com_content&view=article&id=1156:safe2web&catid=9&Itemid=547), l'altra, dal dott. Dicandia "L'accento sulle C" – tre incontri formativi dal titolo "*Tutto in piazza*", "*Bolle in piazza*" e "*Siamo sicuri*" (vedasi http://www.icsfrank-sestosg.gov.it/index.php?option=com_content&view=article&id=1315:formazione-rivolta-ai-genitori-sull-uso-consapevole-di-internet&catid=9&Itemid=547)

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

L'istituto Comprensivo A. Frank dispone di tre laboratori informatici, due collocati nel plesso Frank/Einaudi e uno nella scuola primaria Luini. A questi si aggiungono le LIM presenti in ogni classe di Primaria e Secondaria utilizzate tramite il PC di classe oppure tramite i PC portatili che i docenti della Secondaria hanno in comodato d'uso. In tutti i locali dell'Istituto è presente la rete WiFi. Le infrastrutture sono curate dal docente responsabile del servizio informatico che cura anche il sito web della scuola. I docenti sono responsabili della dotazione tecnologica per il tempo in cui si trovano in classe e in laboratorio.

I compiti del docente Responsabile del servizio informatico sono:

- fornire istruzioni sull'uso delle attrezzature;
- riparare i guasti o malfunzionamenti;
- effettuare controlli periodici del sistema di protezione antivirus

- gestire il sito della scuola
- supportare i docenti nell'utilizzo del registro elettronico
- supportare i docenti nelle prove Invalsi CBT

In generale l'uso delle infrastrutture informatiche è regolamentato dalle seguenti indicazioni:

1) le apparecchiature presenti nella scuola sono patrimonio comune, quindi, vanno utilizzate con il massimo rispetto;
2) i laboratori informatici e le postazioni informatiche dell'istituto possono essere utilizzati esclusivamente per attività di insegnamento, funzionali all'insegnamento e di formazione del personale docente e non docente;
3) l'insegnante che intende usufruire del laboratorio deve obbligatoriamente segnare la prenotazione sul registro delle presenze, indicando il proprio nome, la classe e l'orario di utilizzo;
4) l'ingresso degli allievi nei laboratori è consentito solo in presenza dell'insegnante;
5) è vietato utilizzare dispositivi di massa personali – pendrive o hard disk esterni;
6) all'uscita dai laboratori sarà cura di chi lo ha utilizzato lasciare il locale in ordine e le macchine spente correttamente;
7) in caso di malfunzionamento o guasto dei computer bisogna darne tempestiva segnalazione al responsabile del servizio informatico mediante l'apertura di un ticket;
8) atti di vandalismo o di sabotaggio verranno perseguiti nelle forme previste, compreso il risarcimento degli eventuali danni arrecati.

4. Strumentazione personale

Studenti

La scuola vieta agli studenti l'utilizzo del cellulare e di qualsiasi dispositivo elettronico in orario scolastico.

Secondo il regolamento, esso deve essere spento all'ingresso e rimanere tale per tutto il tempo delle lezioni ed essere riposto nello zaino.

Fanno eccezione gli studenti con disturbi specifici di apprendimento, previa consultazione con il team educativo/Consiglio di classe, concordano le modalità di impiego di strumenti compensativi e le modalità di custodia.

In caso di ripetuta violazione delle suddette disposizioni, il dispositivo dovrà essere consegnato al docente che rileva l'infrazione e che provvederà alla convocazione della famiglia. Il telefono sarà comunque restituito allo studente al termine delle lezioni (vd. Regolamento di disciplina).

I genitori rispondono direttamente dell'operato dei propri figli nel caso in cui, ad esempio, gli stessi arrechino danni ad altre persone a seguito di violazioni della presente policy.

Personale Docente e ATA

"Durante l'orario di servizio sono consentite telefonate per comunicazioni di lavoro come ad es. trovare un collega, segnalare un problema, etc. Le eventuali telefonate private devono essere molto brevi e limitate ai casi di grave necessità. È vietato ogni uso dei dispositivi tecnologici che possa distrarre dai compiti lavorativi per es. l'invio di messaggi e l'uso dei social network." (Circ. n. 12 del 3/10/2017) http://www.icsfrank-sestosg.gov.it/images/Circ_12_Sicurezza_e_privacy.pdf

Nell'invitare tutta la comunità scolastica (studenti, docenti, personale e famiglie) a evitare, per quanto non necessario, la pubblicazione in rete di immagini e/o video ripresi all'interno dell'Istituto (fatta salva la pubblicazione da parte dei docenti in relazione a scopi didattici e/o professionali, previa informativa al Dirigente Scolastico), è bene ricordare che, secondo la normativa vigente, non si possono diffondere immagini, video o foto sul web se non con il consenso delle persone riprese e che la diffusione di filmati e foto che ledono la riservatezza e la dignità delle persone può far incorrere in gravi violazioni, incorrendo in sanzioni disciplinari, pecuniarie ed eventuali reati.

5.PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

5.a Prevenzione

I ragazzi nativi digitali, pur essendo spesso tecnicamente competenti, tendono a non cogliere le implicazioni dei loro comportamenti e tale fenomeno è tanto maggiore quanto è più forte il coinvolgimento emotivo nell'utilizzo dei nuovi media.

Ciò fa sì che alcuni rischi che fanno parte del mondo digitale possano non essere percepiti come tali ed è dunque compito degli adulti, famiglie ed insegnanti, affrontarli con l'obiettivo di prevenirli.

Tra i principali rischi, sia di carattere comportamentale che di matrice tecnica, ricordiamo:

- possibile esposizione a contenuti violenti e non adatti alla loro età;
- videogiochi diseducativi;
- pubblicità ingannevoli;
- possibili contatti con adulti che vogliono conoscere e avvicinare bambini/e o ragazzi/e (adescamento);
- rischio di molestie o maltrattamenti da coetanei (cyber-bullismo);
- scambio di materiale a sfondo sessuale (sexting);
- uso eccessivo di Internet/cellulare (dipendenza).

La scuola interviene pertanto attraverso:

1) l'integrazione nel curricolo dei temi legati al corretto utilizzo delle TIC e di Internet;
2) lo sviluppo di prassi e buone pratiche volte a far riflettere la comunità sull'uso corretto di internet e delle tecnologie digitali;
3) la collaborazione con enti e associazioni per realizzare incontri rivolti a studenti e famiglie con l'intento di fornire elementi utili alla prevenzione e alla gestione dei problemi relativi alla sicurezza informatica;
4) incontri con le forze dell'Ordine per approfondire tematiche sulla legalità e sull'uso consapevole delle Tecnologie;
5) lo "Sportello d'ascolto" rivolto agli alunni della Scuola Secondaria di I grado e della Primaria, uno spazio di ascolto e confronto in cui i ragazzi e le ragazze possono esprimere i propri disagi e le proprie difficoltà all'interno di una relazione d'aiuto ed ottenere informazioni, supporto, consulenza e orientamento;
6) la creazione di un modello di procedura nei casi di bullismo/cyberbullismo.

È responsabilità di ciascun docente inoltre cogliere ogni opportunità per riflettere insieme agli alunni sui rischi in oggetto, nonché monitorare costantemente le relazioni interne alla classe, onde individuare possibili situazioni di disagio ed intervenire tempestivamente, ricorrendo anche a figure specializzate, per sostenere il singolo nelle situazioni e indirizzare il gruppo verso l'instaurazione di un clima positivo, di reciproca accettazione e rispetto.

Tale percorso interno potrà essere ulteriormente rinforzato dalla partecipazione a progetti e/o iniziative esterne coerenti con i temi sopra menzionati, cui la scuola porrà particolare attenzione, selezionando iniziative significative promosse da Enti e/o Associazioni di comprovata affidabilità.

5.b Rilevazione

È compito dell'intera comunità scolastica, l'osservazione e la rilevazione di situazioni critiche che potrebbero dare adito a casi di bullismo e cyberbullismo. A partire dalla corretta formazione e sensibilizzazione di tutti gli adulti coinvolti, docenti e personale ATA sono invitati a essere confidenti e custodi, diretti o indiretti, di ciò che le ragazze e i ragazzi vivono. Si raccomanda di evitare ogni atteggiamento accusatorio o intimidatorio per riuscire a ricevere, dai minori più fragili, segnalazioni e confidenze circa situazioni problematiche vissute.

Gli insegnanti sono chiamati a ricoprire un ruolo estremamente delicato ma di grande responsabilità nell'individuazione e osservazione delle problematiche, dei rischi, dei pericoli che bambine, bambini e adolescenti possono vivere e affrontare ogni giorno. Accorgersi tempestivamente di quanto accade e compiere azioni immediate di contrasto verso gli atti inopportuni, quando non illegali, diviene fondamentale per poter evitare conseguenze che possano pregiudicare il benessere e una crescita armonica dei soggetti coinvolti.

Il bullismo è un fenomeno ormai noto a scuola e viene definito come *il reiterarsi di comportamenti e atteggiamenti diretti o indiretti volti a prevaricare un altro con l'intenzione di nuocere, con l'uso della forza fisica o della prevaricazione psicologica*.

Per potere parlare di bullismo dobbiamo essere in presenza di:
- prepotenze intenzionali e soprusi che avvengono per lo più in un contesto di gruppo
- azioni continuative e persistenti
- azioni che mirano deliberatamente a danneggiare qualcuno in vari modi: verbale, fisico o psicologico
- disparità di forze tra chi attacca e chi subisce: la persona oggetto di prepotenze non è capace di difendersi da sola

Non si può parlare di bullismo per singoli episodi di prepotenza, di tipo del tutto OCCASIONALE. Questi possono essere anche molto gravi, ma rientrano in altre tipologie di comportamento: SCHERZO / LITIGIO / REATO.

Il cyberbullismo o bullismo elettronico consiste nell'uso di internet o altre tecnologie digitali finalizzato a insultare o minacciare qualcuno e costituisce una modalità di intimidazione pervasiva che può sperimentare qualsiasi adolescente che usa i mezzi di comunicazione elettronici.

Le principali tipologie di cyberbullismo sono state classificate nel modo seguente:

Flaming: un flame (termine inglese che significa "fiamma") è un messaggio deliberatamente ostile e provocatorio inviato da un utente alla comunità o a un singolo individuo; il flaming avviene tramite l'invio di messaggi elettronici, violenti e volgari allo scopo di suscitare conflitti verbali all'interno della rete tra due o più utenti.
Harassment: caratteristica di questa tipologia di cyberbullismo sono le molestie, ossia azioni, parole o comportamenti, persistenti e ripetuti, diretti verso una persona specifica, che possono causare disagio emotivo e psichico. Come nel bullismo tradizionale, si viene a creare una relazione sbilanciata, nella quale la vittima subisce passivamente le molestie, o al massimo tenta, generalmente senza successo, di convincere il persecutore a porre fine alle aggressioni.
Cyberstalking: questo termine viene utilizzato per definire l'invio ripetuto di messaggi che includono esplicite minacce fisiche, al punto che la vittima arriva a temere per la propria incolumità.
Denigration: distribuzione, all'interno della rete o tramite SMS, di messaggi falsi o dispregiativi con pettegolezzi e commenti crudeli, calunniosi, denigratori nei confronti delle vittime, con lo scopo "di danneggiare la reputazione o le amicizie di colui che viene preso di mira".
Impersonation: caratteristica di questo fenomeno è che il persecutore si crea un'identità fittizia con il nome di un'altra persona nota, usando una sua foto, creando un nuovo profilo parallelo, fingendo di essere quella persona per poi parlare male di qualcuno, offendere,

farsi raccontare cose. Può anche accadere che il soggetto intruso, se in possesso del nome utente e della password della vittima, invii dei messaggi, a nome di questa, ad un'altra persona, che non saprà che i messaggi che gli sono arrivati non sono, in realtà, stati inviati dal proprio conoscente, ma da qualcuno che si è impossessato della sua identità. In certi casi, il bullo modifica la password della vittima, impedendogli così l'accesso alla propria mail o account. Questa forma di aggressione può creare problemi o, addirittura, mettere in pericolo il vero proprietario dell'account.
Trickery e Outing: la peculiarità di questo fenomeno risiede nell'intento di ingannare la vittima: il bullo tramite questa strategia entra prima in confidenza con la vittima, scambiando con essa informazioni intime e/o private, e una volta ottenute le informazioni e la fiducia, le diffonde tramite mezzi elettronici come internet, sms, etc.
Exclusion: consiste nell'escludere intenzionalmente un altro utente dal proprio gruppo di amici, dalla chat o da un gioco interattivo. L'esclusione dal gruppo di amici è percepita come una grave offesa, che è in grado di ridurre la popolarità tra il gruppo dei pari.
Sexting: invio di messaggi via smartphone e internet, corredati da immagini a sfondo sessuale.

Laddove il docente colga possibili situazioni di disagio connesse ad uno o più di uno tra i rischi elencati nel paragrafo "Prevenzione", potrà chiedere il supporto dei docenti referenti, del coordinatori di classe, del Dirigente Scolastico e della psicologa che gestisce lo Sportello di ascolto della scuola, sia sulla base di eventi osservati direttamente a scuola, sia su eventi particolari che gli sono stati confidati dall'alunno o comunicati da terzi.

5.c Gestione dei casi

La gestione dei casi rilevati va differenziata a seconda della loro gravità. È sempre opportuna la condivisione a livello di Consiglio di Classe di ogni episodio rilevato. Alcuni avvenimenti potranno essere discussi e risolti in classe; altri invece dovranno essere affrontati convocando genitori e alunno/a per riflettere insieme su quanto accaduto e come rimediare. Nei casi più gravi e in ogni ipotesi di reato occorre valutare tempestivamente con il Dirigente Scolastico come intervenire. Per chiarire cosa fare in caso di sospetta situazione di bullismo/cyberbullismo, si rinvia al modello di procedura nel protocollo di intervento

A seguito della segnalazione, verrà avviato un colloquio finalizzato a valutare la necessità di effettuare uno o più interventi di osservazione in classe e, successivamente, di pianificare adeguati interventi educativi e, ove necessario, di coinvolgere le famiglie per l'attivazione di un percorso comune e condiviso di sostegno al disagio. Le azioni poste in essere dalla scuola saranno dirette non solo a supportare le vittime, le famiglie e tutti coloro che sono stati spettatori attivi o passivi di quanto avvenuto, ma anche a realizzare interventi educativi rispetto a quanti abbiano messo in atto comportamenti lesivi, ove si tratti di soggetti interni all'Istituto. Nei casi di maggiore gravità si valuterà anche il coinvolgimento di attori esterni quali le forze dell'ordine e i servizi sociali.

Schema procedure scolastiche in caso di atti di cyberbullismo

Quando si viene a conoscenza di un atto che potrebbe essere configurabile come cyberbullismo Informazione immediata al Dirigente Scolastico

1^ Fase: analisi e valutazione

- Soggetti responsabili: Dirigente Scolastico e docenti del Consiglio di classe
- Altri soggetti coinvolti: Referente cyberbullismo / Psicologo della scuola
- Raccolta di informazioni sull'accaduto: quando è successo, dove, con quali modalità
- Interviste e colloqui con gli attori principali, i singoli, il gruppo; vengono raccolte le diverse versioni e ricostruiti i fatti ed i punti di vista.

In questa fase è importante astenersi dal formulare giudizi; è piuttosto necessario creare un clima di empatia, di solidarietà e di disponibilità al confronto che permetta un'oggettiva raccolta di informazioni; l'adulto è un mediatore in un contesto neutro.

2^ Fase: risultati sui fatti oggetto di indagine

Soggetti responsabili: Dirigente Scolastico e docenti del Consiglio di classe

Altri soggetti coinvolti: Referente cyberbullismo / Psicologo della scuola

- I fatti sono confermati / esistono prove oggettive Vengono stabilite le azioni e provvedimenti disciplinari da intraprendere
- I fatti non sono configurabili come cyberbullismo Non si ritiene di intervenire in modo specifico; prosegue il compito educativo

3^ Fase: azioni e provvedimenti

Se i fatti sono confermati:

- Comunicazione ai genitori della vittima da parte del docente coordinatore (convocazione scritta o telefonica) e supporto di tutto il consiglio di classe nell'affrontare la situazione segnalata, concordando modalità di soluzione e analizzando le risorse disponibili dentro e fuori della scuola (psicologo, medico, altri…);

- Comunicazione ai genitori del cyberbullo (convocazione)
- Convocazione del Consiglio di classe e valutazione del tipo di provvedimento disciplinare, secondo la gravità:

    - sospensione del diritto a partecipare ad uscite didattiche;
    - sospensione con obbligo di frequenza con svolgimento di lavori socialmente utili o studio individuale, con verifica finale, sulle tematiche del rispetto dell'altro;
    - sospensione senza obbligo di frequenza;

- Invito al cyberbullo allo svolgimento di azioni positive, per es. lettera di scuse alla vittima;

- Nei casi più gravi denuncia o segnalazione ad un organo di polizia o all'autorità giudiziaria (Questura, Carabinieri, ecc.) per attivare un procedimento penale (eventuale querela di parte);

- Nel caso in cui la famiglia non collabori, minimizzi, mostri atteggiamenti oppositivi o comunque inadeguatezza, debolezza educativa o sia recidiva nei comportamenti: segnalazione ai Servizi Sociali del Comune.

4^ Fase: percorso educativo e monitoraggio

Il Dirigente, i docenti del Consiglio di classe e gli altri soggetti coinvolti:

- si occupano del rafforzamento del percorso educativo all'interno della classe e/o del gruppo coinvolto;

- provvedono al monitoraggio del fenomeno e della valutazione dell'intervento attuato sia nei confronti del cyberbullo, sia nei confronti della vittima.