



I.C. "Galileo Ferraris"

Scuole di Livorno Ferraris, Saluggia, Sant'Antonino

LIVORNO FERRARIS – 13046 - Viale IV Novembre, 16
Tel - 0161 47236 / 271, 421577 – CF 93005220020
vcic80500n@istruzione.it – vcic80500n@pec.istruzione.it
<http://www.istitutocomprensivolivornoferraris.it>



Anno scolastico 2019-20

E-SAFETY POLICY D'ISTITUTO



Questo documento integra per obiettivi e contenuti, nello specifico in relazione alle politiche dell'uso della rete, i documenti che specificano le politiche dell'Istituto

(il PTOF, incluso il piano per l'attuazione del PNSD e il Regolamento Interno d'Istituto)

Sommario

1-	Introduzione: Scopi della Policy	3
2-	Ruoli e Responsabilità	3
3-	Gestione delle infrazioni della Policy e dei comportamenti a rischio	5
4-	Formazione e Curricolo.....	5
	<i>Curricolo sulle competenze digitali per gli studenti.</i>	5
	<i>Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica e sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali</i>	5
	<i>Sensibilizzazione delle famiglie</i>	6
5-	Strumentazione personale	6
6-	Prevenzione, rilevazione e gestione dei casi	6
	<i>Prevenzione</i>	6
	<i>Azioni</i>	7
	<i>Rilevazione</i>	7
	<i>Gestione dei casi</i>	7
	ALLEGATO A: procedure operative per la protezione dei dati personali	9
	Allegato B: procedure operative per la gestione delle infrazioni alla e-policy.	11
Allegato C:	procedure operative per la rilevazione, il monitoraggio e la gestione delle segnalazioni e dei casi.	14
Allegato D:	documento di e-safety policy consenso dei genitori/tutori per l'accesso ad internet e dichiarazione liberatoria per la pubblicazione di elaborati, nomi, voci, immagini, materiale audiovisivo... ..	15
Allegato E:	documento di e-safety policy assunzione di responsabilità da parte di docenti e altro personale della scuola.....	16
Allegato F-1:	POLITICA DI USO ACCETTABILE DELLA RETE - Per gli alunni fino a 9 anni	17
Allegato F-2:	POLITICA DI USO ACCETTABILE DELLA RETE - Per gli alunni dai 9 agli 11 anni.....	18
Allegato F-3:	POLITICA DI USO ACCETTABILE DELLA RETE- Per gli alunni dagli 11 ai 14 anni.....	19

1- Introduzione: Scopi della Policy

In attuazione della **Legge 71/2017 art. 1**, l'I.C. *Galileo Ferraris*, predispone la presente policy di E-safety per garantire l'attuazione degli interventi per contrastare il fenomeno del cyberbullismo in tutte le sue manifestazioni e rendere tutti più consapevoli nell'uso degli strumenti odierni di comunicazione informatica.

Ricordiamo infatti che la sicurezza e l'utilizzo consapevole delle TIC richiede, da parte di tutti i docenti, la profonda conoscenza di tutte le modalità, strumenti, azioni e conseguenze che si esplicitano attorno a questo nuovo universo parallelo, soprattutto in relazione alle potenzialità e ai rischi della rete e dei social network.

Partendo dal presupposto che le tecnologie non rappresentano un demone, ma sono un'opportunità di crescita, di conoscenza, di relazione, di auto-imprenditorialità, di realizzazione, occorre, per conseguire questo obiettivo, formare docenti, alunni e famiglie a un loro utilizzo consapevole, adeguato e proficuo.

Bisogna imparare ad evitare l'utilizzo improprio, perché inconsapevole, di posta elettronica, messaggistica istantanea, blog, sms, WhatsApp e altre modalità social che possono veicolare contenuti "dannosi" e/o "diffamatori".

Occorre formare e sensibilizzare docenti, genitori e alunni su atteggiamenti, relazioni, approcci che apparentemente vengono giustificati e argomentati come "leggerezze" o "scherzi", ma che possono essere invece, talvolta, azioni capaci di denigrare, diffamare e ferire l'individualità e la personalità dell'altro, in un ambiente i cui confini sono globali.

Bullismo e cyberbullismo sono i pericoli attuali legati alla condizione sociale e tecnologica del nostro tempo.

La Scuola ha come finalità non solo la formazione didattica e culturale degli studenti, ma anche intenti educativi e formativi che si esplicano attraverso la trasmissione di valori quali il rispetto dell'altro e la costruzione di relazioni "sane", prive di vessazioni, discriminazioni, atti di violenza.

Promuovere l'acquisizione di abilità pro-sociali e relazionali basate sul rispetto, sull'empatia e non sull'abuso di potere e sul desiderio di intimidire e di dominare è compito di tutti coloro che si occupano a vario titolo dell'educazione dei bambini e degli adolescenti.

2- Ruoli e Responsabilità

Il Dirigente nomina il referente nonché i membri del gruppo di lavoro per il contrasto al bullismo e al cyberbullismo: per garantire la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri della comunità scolastica; per garantire ai 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; per garantire l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza on line.

È il dirigente Scolastico che regola il comportamento degli studenti, propone azioni correttive in caso di comportamento inadeguato, in stretta collaborazione con i consigli di classe.

Presso l'I.C. *Galileo Ferraris*, il Dirigente ha individuato fra i docenti un referente, con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo. L'istituto potrà avvalersi in tal senso della collaborazione delle Forze dell'Ordine nonché delle associazioni e dei centri di aggregazione giovanile presenti sul territorio.

Il referente, formato attraverso la piattaforma Sofia e corsi specifici di aggiornamento, promuove l'adesione all'iniziativa "Generazioni connesse". Sarà coadiuvato da docenti selezionati per plesso e ordine di scuola, che costituiranno il **gruppo di lavoro per il Contrasto al Bullismo e al Cyberbullismo**.

In particolare, il **Referente per il cyberbullismo d'Istituto**:

- coordina iniziative di prevenzione e contrasto del cyberbullismo messe in atto dalla scuola;

- Predisporre un documento di rilevazione di incidenti di sicurezza in rete e negli ambienti scolastici;
- Facilita la formazione e la consulenza di tutto il personale.

Spetta invece all'Animatore Digitale e Team dell'Innovazione:

- La pubblicazione del documento di E-Safety Policy sul sito della scuola;
- La diffusione dei contenuti del documento tra docenti e studenti.

Gli Insegnanti:

- provvedono personalmente alla propria formazione/aggiornamento sull'utilizzo del digitale con particolare riferimento alla dimensione etica (tutela della privacy, rispetto dei diritti intellettuali dei materiali reperiti in Internet e dell'immagine degli altri: lotta al cyberbullismo);
- supportano gli alunni nell'utilizzo consapevole delle tecnologie informatiche utilizzate a scopi didattici;
- segnalano al Dirigente scolastico e ai suoi collaboratori eventuali episodi di violazione delle norme di comportamento stabilite dalla scuola, avviando le procedure previste in caso di violazioni;
- supportano ed indirizzano alunni coinvolti in problematiche legate alla rete.

Gli Alunni:

- leggono comprendono ed accettano il documento di E-Safety Policy;
- comprendono e rispettano le norme sul diritto d'autore;
- prendono consapevolezza delle situazioni di rischio legate alla rete, telefoni cellulari, fotocamere digitali;
- si responsabilizzano in merito alla politica della scuola sull'uso delle immagini;
- comprendono l'importanza di adottare buone pratiche di sicurezza on-line quando si usano le tecnologie;
- si assumono la responsabilità di un utilizzo sbagliato delle tecnologie.

Il Referente TIC:

- può controllare ed accedere a tutti i files della rete intranet;
- è l'unico a poter installare nuovi software;
- limita attraverso un proxy l'accesso ad alcuni siti;
- gestisce la prenotazione dei laboratori, tramite registro, che consente di tenere traccia di ora e laboratorio utilizzati da ciascuno.

Il Direttore dei Servizi Generali e Amministrativi:

- assicura, nei limiti delle risorse finanziarie disponibili, gli interventi di manutenzione necessari ad evitare un cattivo funzionamento della dotazione tecnologica dell'Istituto, controllando al contempo che le norme di sicurezza vengano rispettate;

I Genitori:

- contribuiscono, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete;
- incoraggiano l'impiego delle ICT da parte degli alunni se utili allo svolgimento dei compiti a casa, controllando che tale impiego avvenga nel rispetto delle norme di sicurezza;
- agiscono in modo concorde con la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite;
- rispondono per gli episodi, soprattutto se gravi, commessi dai figli minori a titolo di culpa in educando (articolo 2048 del Codice civile). Sono esonerati da responsabilità solo se dimostrano di non aver potuto impedire il fatto.

La presente Policy di e-safety verrà pubblicata sul sito della scuola e condivisa in primo luogo con i docenti dell'Istituto Comprensivo nel Collegio docenti di ottobre 2019.

È già stato chiesto ai docenti di partecipare attivamente alla comprensione e diffusione dello stesso.

3- Gestione delle infrazioni della Policy e dei comportamenti a rischio

In caso di rilevazione di comportamenti a rischio che si possano configurare o non come reati, il docente che ne venga a conoscenza, fermi in ogni caso gli obblighi di legge a suo carico, è tenuto a rivolgersi in primo luogo al Referente d'Istituto per il contrasto al bullismo e al cyberbullismo, che a sua volta ha il compito di coordinare le iniziative da mettere in atto (art. 3 comma 3 legge 71/2017) e informare il Dirigente Scolastico.

Il Dirigente, sentiti i soggetti sopra citati e acquisiti gli elementi necessari alla valutazione delle circostanze di fatto, convoca i genitori/tutori legali degli studenti coinvolti; in ogni caso il Dirigente si riserva, ove ritenuto necessario, le segnalazioni alle autorità competenti, come previsto dall'art. 5 della Legge 71/2017.

I provvedimenti da adottare da parte del consiglio di classe nei confronti dell'alunno che ha commesso un'infrazione alla policy (in proporzione sia all'età dello studente sia alla gravità dell'infrazione commessa) potranno essere:

- richiamo verbale;
- azioni estemporanee commisurate alla gravità della violazione commessa (assegnazione di attività aggiuntive da svolgere a casa su temi di Cittadinanza e Costituzione; sequestro dello strumento informatico o comunicativo usato, etc);
- nota informativa ai genitori o tutori mediante registro elettronico e/o diario;
- convocazione dei genitori o tutori per un colloquio con l'insegnante;
- convocazione dei genitori o tutori per un colloquio con il Dirigente scolastico nel quale verranno definite azioni correttive: lavori socialmente utili alla scuola e all'alunno (es. catalogazione libri biblioteca, lettura di testi aggiuntivi, attività di studio individuale su specifici argomenti o collaborazione con il personale) nelle ore/giorni di sospensione dalle attività didattiche con obbligo di frequenza; eventualmente anche rientro pomeridiano a scuola per attività di peer tutoring nelle scuole di grado inferiore.

Per il **Monitoraggio dell'implementazione della Policy e suo aggiornamento nel corso dei prossimi anni, verrà costituita apposita commissione** che presenterà una relazione di monitoraggio al Collegio Docenti del mese di giugno di ogni anno, la relazione sarà presentata dal referente. Saranno ben accette le proposte dei genitori che verranno vagliate dalla commissione stessa.

All'avvio del nuovo anno scolastico si prevede un'azione di revisione ed eventuale aggiornamento del documento.

4- Formazione e Curricolo

[Curricolo sulle competenze digitali per gli studenti.](#)

All'interno delle prassi didattiche per migliorare l'ambiente di apprendimento e garantire il successo formativo di tutti gli allievi e diminuire il rischio di insuccesso scolastico, si opera per integrare il curricolo inserendo la conoscenza, l'acquisizione e l'utilizzo delle TIC in modo trasversale e interdisciplinare.

Le nuove tecnologie devono divenire strumento e modalità di costruzione del sé e di relazione con gli altri dobbiamo quindi pensare alle TIC come: canale, mezzo, strumento e forma di rappresentazione; le nuove tecnologie possono mediare le relazioni al contempo si possono educare i nuovi cittadini ad avere delle relazioni consapevoli con le tecnologie.

Le competenze digitali, come espresso dalla legge 107/2015, sono finalizzate all'uso critico e consapevole anche dei social e dei media (PNSD).

[Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica e sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali](#)

L'istituto ha già attivato, anche in rete, corsi di formazione sull'utilizzo degli strumenti informatici (Robotica e coding, competenze digitali) e incentiva la partecipazione a corsi di aggiornamento legati alle nuove tecnologie, all'intercultura, ai bisogni educativi speciali.

La scuola nell'a.s. 2019/20 ha permesso al referente del bullismo e cyberbullismo di frequentare specifici corsi di formazione on line e in presenza.

Il referente ha il compito di promuovere la diffusione delle informazioni attraverso la condivisione di materiale tramite il registro elettronico o altre piattaforme. Si intendono promuovere incontri di formazione per i docenti interni per la condivisione di spunti e materiali intorno alla Legge 71/2017 e della bibliografia, filmografia e sitografia utile per la costruzione di unità di apprendimento e attività didattiche su bullismo/cyberbullismo.

Sensibilizzazione delle famiglie

All'inizio di ogni anno scolastico, è previsto un incontro conoscitivo rivolto a tutti i genitori/tutori degli studenti (per classi parallele) con il Referente, il gruppo di lavoro per il contrasto al Bullismo e al Cyberbullismo e/o esperti nel settore che illustreranno le iniziative di formazione e sensibilizzazione intraprese dalla scuola allo scopo di collaborare con la componente genitori per l'educazione a un uso consapevole delle nuove tecnologie e alla valutazione delle situazioni di rischio.

La condivisione con le famiglie degli studenti del Regolamento di Prevenzione e Contrasto del Bullismo e del Cyberbullismo, avverrà sia via mail che in occasione della condivisione del Patto di Corresponsabilità.

La presente E-policy e il Regolamento di Prevenzione e Contrasto del Bullismo e del Cyberbullismo, verranno pubblicati anche nel sito istituzionale della scuola.

5- Strumentazione personale

Per gli studenti il Regolamento scolastico non consente l'utilizzo del cellulare durante le lezioni, ma lo favorisce, insieme ad altri device, solo in alcuni momenti di apprendimento cooperativo, ricerca, condivisione file e accessi alle piattaforme di classe sotto la supervisione dei docenti, nonché nel caso gli stessi strumenti siano previsti quali compensativi (PEI-PDP).

Per i docenti: la scuola mette a disposizione una postazione e favorisce accesso a Internet tramite rete Wi-Fi.

L'uso di dispositivi elettronici personali è permesso solo per attività funzionali al servizio.

6- Prevenzione, rilevazione e gestione dei casi

Prevenzione

In linea con quanto disposto dall'art. 5 comma 5 della Legge 71/2017, l'I.C. Galileo Ferraris promuove *«l'educazione all'uso consapevole della rete internet e ai diritti e doveri connessi all'utilizzo delle tecnologie informatiche, quale elemento trasversale alle diverse discipline curricolari, anche mediante la realizzazione di apposite attività progettuali aventi carattere di continuità tra i diversi gradi istruzione o di progetti elaborati da reti di scuole in collaborazione con enti locali, servizi territoriali, organi di polizia, associazioni ed enti»*.

Tra le attività avviate e i progetti in corso si possono segnalare:

- La condivisione materiali didattici sul contrasto al Bullismo e cyberbullismo.
- La progettazione costante di attività didattiche per il potenziamento delle competenze sociali e civiche e delle competenze socioaffettive, di attività in apprendimento cooperativo, di attività per il riconoscimento e il rispetto delle differenze.
- Attività di formazione all'utilizzo consapevole delle TIC attraverso il potenziamento delle competenze digitale e la sensibilizzazione alla sicurezza in rete.
- Attività specifiche intorno al bullismo e al cyberbullismo come contenuto di riflessione.
- L'intento di attivare una costante formazione per i genitori e le famiglie degli studenti.
- Incontri conoscitivi con le forze dell'ordine (Polizia Postale e delle comunicazioni, Guardia di Finanza, Carabinieri), nell'ambito dei progetti previsti dal PTOF riguardanti l'educazione alla legalità.

Attraverso la formazione si intende prevenire e gestire il rischio di eventi di Bullismo e Cyberbullismo.

In particolare, vengono evidenziate le seguenti **responsabilità dei docenti** che debbono:

- Saper riconoscere i rischi più comuni che i ragazzi possono correre sul web, per potere poi intervenire adeguatamente.
- Monitorare situazioni (Referente-Docenti- Personale scolastico)
- Attuare percorsi scolastici di educazione all'affettività, educazione alla cittadinanza ed alla convivenza civile, educazione al rispetto, educazione all'uso consapevole della rete, incontri con istituzioni.
- Illustrare in attività didattiche le tipologie di cyberbullismo, così come in parte riportato nell'integrazione al Regolamento d'Istituto.

Azioni

Si aderirà alla **piattaforma Generazioni connesse**:

- sarà individuato un gruppo di lavoro rappresentativo dei tre ordini di scuola nei due comuni facenti parte dell'Istituto, con l'obiettivo di redigere eventuali aggiornamenti e modifiche della e-policy, elaborare strategie di rilevazione del fenomeno del bullismo e del cyberbullismo, progettare la condivisione delle buone pratiche sull'uso consapevole delle nuove tecnologie con il corpo docente e i genitori, individuare strumenti e progettare interventi per il potenziamento delle competenze di cittadinanza e di socio-affettività;
- verrà svolto un primo incontro di formazione curato del gruppo di lavoro per i docenti interni per riflettere intorno alla Legge 71/2017;
- verrà predisposta una comunicazione sul sito web della scuola sulla somministrazione del questionario bullismo/cyberbullismo, solo dopo aver informato i rappresentanti dei genitori di tutti i consigli di classe della partecipazione della scuola al progetto Generazioni Connesse.

Il nostro Istituto ha già avviato azioni formative con le forze dell'ordine, nell'ambito dei progetti previsti dal PTOF riguardanti l'educazione alla legalità e il potenziamento delle competenze sociali e civiche.

Rilevazione

Saranno elaborati questionari di rilevazione del fenomeno del bullismo e del cyberbullismo sulla base delle indicazioni ministeriali e del modello di Olweus¹ e di Sharp e Smith, diversificati per ordine di scuola, riportati in coda al presente documento.

I questionari, anonimi, verranno somministrati ogni anno, tramite la piattaforma digitale, alle classi IV e V della Scuola Primaria e I e II della Secondaria di I grado.

Viene individuato un format per la segnalazione e gestione di eventuali casi e una procedura di gestione degli stessi e della definizione delle azioni da intraprendere a seconda del caso.

Gestione dei casi

Nel caso di individuazione di comportamenti a rischio o atti di cyberbullismo, dopo opportuna indagine si provvede al coinvolgimento delle famiglie e si procede alla convocazione di un Consiglio di classe.

Accanto ad eventuali azioni previste dal Regolamento, si attiveranno ulteriori percorsi didattici e iniziative educative di potenziamento delle competenze socioaffettive e, quando necessario, di peer tutoring, eventualmente anche in collaborazione con le autorità

¹ Lo strumento più classico per rilevare la presenza di comportamenti di bullismo e corrispondente vittimismo è un questionario piuttosto semplice, utilizzato sia in Italia che all'estero dalla quarta elementare alla terza media. Si compone di 28 domande divise in due parti, una relativa alla prepotenza subita e l'altra alla prepotenza agita.

competenti e i servizi sociali, necessari ad affrontare adeguatamente la questione con i soggetti nel contesto delle classi.

Referente Scolastico

Chiara Michelone

Dirigente Scolastico

Maria Lina La China

ALLEGATO A: procedure operative per la protezione dei dati personali

Ognuno ha il diritto di impedire che le proprie informazioni personali (numero di telefono, indirizzo, ma anche scuola che si frequenta, foto personali, ecc...) diventino note ad altri.

È quello che si intende per "diritto alla privacy".

Saperlo riconoscere, gestire e difendere è il primo passo per navigare in Rete in modo responsabile.

L'istituto comprensivo si impegna a:

- ✓ Utilizzare i dati personali lealmente e legalmente;
- ✓ per i fini specificamente dichiarati e limitati;
- ✓ in modo adeguato, accurato, pertinente e non eccessivo;
- ✓ vengono conservati solo per il tempo strettamente necessario e manipolati rispettando i diritti di protezione della privacy;
- ✓ sono mantenuti sicuri e protetti;
- ✓ non trasferiti al di fuori dello spazio della Comunità europea senza adeguata protezione.

I docenti si impegnano a:

- ✓ Non comunicare mai le proprie password a nessuno, tantomeno agli studenti;
- ✓ Nella navigazione online, assicurarsi di negare sempre il consenso ad ogni richiesta di salvare le password utilizzate;
- ✓ Utilizzare una pen drive per lavorare sui PC comuni della scuola, evitando di salvare nella memoria interna del PC;
- ✓ Prima di lasciare una postazione comune, assicurarsi di aver cancellato ogni file scaricato o elaborato su quella postazione;
- ✓ Si avvisa che l'Animatore Digitale ed il Team, periodicamente, cancelleranno files e password salvate accidentalmente sui PC comuni della scuola e pertanto i dati potranno andar persi.

Gli alunni

Si impegnano a

- ✓ pensare prima di eventualmente inviare qualsiasi tipo di file, e chiedersi se sta condividendo o inviando cose a rischio-pentimento. Per sicurezza, dovrebbe domandarsi proprio: *"E' sicuro che voglio dirlo o mostrarlo proprio a tutti?"*. *"Tra qualche tempo potrei cambiare idea per qualche motivo?"*. Se la risposta è anche un pò incerta, vale la pena fermarsi.
- ✓ Decidere prima, magari con l'aiuto di un adulto, le cose che si possono condividere o inviare, e quelle che vanno tenute sempre fuori dalla rete, come le informazioni troppo personali, l'indirizzo, il telefono o il nome della scuola etc.
- ✓ Gestire le impostazioni delle App e social network selezionando un adeguato livello di privacy.
- ✓ Non stare troppo su internet o sui social e nei profili online non condividere troppe informazioni (comprese foto o video).
- ✓ Scaricare le app consapevolmente perché possono essere collegate ad esempio a un sistema di geolocalizzazione.
- ✓ Bloccare e segnalare siti internet o social network che diffondono video o altri documenti tutelati dalla privacy.

Consigli per rispettare la privacy degli altri

- ✓ Non diffondere informazioni personali di altri.
- ✓ Fare in modo che gli altri rispettino la tua privacy e rispetta sempre la loro.
- ✓ Prima di taggare chiedere il permesso, infatti prima di pubblicare una foto su un social dovresti chiedere alle persone che vi compaiono un specifica autorizzazione.

- ✓ Rispetta sempre un'etichetta di comportamento corretto e rispettoso (Non scrivere messaggi cattivi, e non girare foto o info contro qualcuno, neanche se pensi sia per scherzo: potresti partecipare a un'azione di cyberbullismo, magari senza accorgertene)

I genitori

- ✓ Educano al rispetto sia offline che online e promuovono comportamenti relazionali positivi in famiglia e fuori: i figli fanno riferimento, prima di tutto, ai modelli che imparano dai genitori anche sull'uso delle tecnologie.
 - ✓ Partecipano alle attività che il figlio/a svolge online, impegnandosi a conoscere non solo i contatti e i social a cui è iscritto/a, ma anche cosa fa, cosa lo/la interessa o appassiona online.
 - ✓ Stabiliscono insieme alcune semplici regole di sicurezza da seguire sempre. Per esempio, non accettare inviti o amicizie sui social network da parte di sconosciuti, si informano se c'è qualcuno che inopportuna online, eccetera.
 - ✓ Prestano attenzione anche ai piccoli cambiamenti che avvengono nel comportamento e negli atteggiamenti del proprio figlio (non vuole più frequentare scuola o luoghi abitualmente frequentati, o si mostra preoccupato o in ansia ad ogni notifica che riceve sui social). Solo così possono accorgersi se qualcosa lo/la turba.
 - ✓ Dialogano: mostrano al proprio figlio/a la disponibilità ad ascoltare e creano le condizioni affinché – qualora sorgano problemi – si senta libero/a di condividere le sue preoccupazioni, sicuro/a di trovare interlocutori attenti e non giudicanti.
 - ✓ Prima di postare anche sulle chat tra genitori, riflettono sulle possibili problematiche che si verrebbero ad innescare, aiutando in tal modo, con l'esempio, il proprio figlio a fare lo stesso, cioè a riflettere prima di scrivere/postare/inoltrare.
- Purtroppo il Web non dimentica e spesso la diffusione è immediata e virale.

Allegato B: procedure operative per la gestione delle infrazioni alla E-Policy.

Procedure operative per la gestione delle infrazioni alla E-Policy.

1. Se si tratta di un docente:

- Segnalare all'Animatore Digitale o al referente del bullismo e Cyberbullismo.
- Loro valuteranno se intervenire personalmente solo nei casi più lievi.
- Nei casi più gravi se riferire alla Dirigente.

2. Se si tratta di un alunno:

- Segnalare all'Animatore Digitale o al referente del bullismo e Cyberbullismo;
- Loro valuteranno se intervenire personalmente, con il coordinatore di classe, solo nei casi più lievi con colloqui con i genitori in presenza della dirigente.
- Nei casi più gravi sarà necessario confrontarsi con il Consiglio di Classe, l'Animatore Digitale, il referente al bullismo e Cyberbullismo e valutare, con la dirigente, le azioni da intraprendere con riferimento al Regolamento d'Istituto.

Ogni volta che un membro della comunità educante viola la E-Safety Policy, la decisione sul livello di azione che verrà applicata è affidata agli organi competenti.

Laddove se ne valuti la necessità si farà riferimento anche alle norme generali di comportamento, del contratto e della giurisprudenza, già in essere e sempre valide, nonché alle relative procedure.

La decisione finale sul livello di azioni sarà validata dal Dirigente Scolastico e rifletterà le procedure comportamentali e disciplinari della scuola.

L'E-Safety Policy della scuola sarà resa disponibile ai genitori che dovranno firmare un modulo di accettazione.

Come ci si farà carico delle infrazioni dello studente/gli studenti e per i membri della comunità scolastica che infrangono la e-Safety Policy?

STUDENTI

Infrazioni: Categoria A	Organo competente e azioni possibili:
<ul style="list-style-type: none">L'uso di siti non-educativi durante le lezioni.L'utilizzo non autorizzato di e-mail. L'uso non autorizzato del telefono cellulare (o altre nuove tecnologie) durante le lezioni.Uso di instant messaging / siti di social networking	<p>Fare riferimento all'insegnante della classe/ Referente bullismo/Dirigente Scolastico</p> <p>Nota disciplinare sul registro di classe che nel secondo caso può essere aumentata con: segnalazione al dirigente scolastico</p>
Infrazioni: Categoria B	Organo competente e azioni possibili:
<ul style="list-style-type: none">L'uso continuato di siti non-educativi durante le lezioni <u>dopo essere stato avvertito</u>.L'uso non autorizzato di e-mail dopo essere stato avvertito.L'uso non autorizzato del telefono cellulare (o altre nuove tecnologie) dopo essere stato avvertito.L'uso continuato messaggistica / chat room istantanea, siti di social networking, newsgroup.L'uso di materiale offensivo.	<p>Fare riferimento all'insegnante della classe/ Referente bullismo/Dirigente Scolastico</p> <p>Nota disciplinare sul registro di classe</p> <p>Può essere aumentata con: segnalazione al dirigente scolastico</p> <p>Escalation a:</p> <ol style="list-style-type: none">rimozione di telefono fino a fine giornata;contatto con i genitori e successiva contestazione di addebito per svolgere "lavori utili".
<p><u>In caso di: uso non autorizzato di dispositivi elettronici durante una verifica scritta per copiare</u></p>	<p>Ritiro della verifica e valutazione gravemente insufficiente della stessa. Nota sul registro di classe</p>

<u>e/o reperire informazioni uso non autorizzato durante gli esami</u>	(registro elettronico) e comunicazione alla famiglia su diario. Immediata sospensione della prova e provvedimenti dettati dalle linee guida per gli Esami di stato che confluiscono in una bocciatura.
Infrazioni: Categoria C	Organo competente e azioni possibili:
Rovinare o distruggere deliberatamente i dati di qualcuno, violare la privacy altrui o messaggi inappropriati, video o immagini su un sito di social networking. <ul style="list-style-type: none"> • Invio di un messaggio e-mail o MSN che è considerato molestia o azione di bullismo. • Cercare di accedere a materiale offensivo o pornografico. 	Fare riferimento all'insegnante della classe/ Referente bullismo/Dirigente Scolastico Escalation a: 1. rimozione del telefono fino a fine giornata; 2. contatto con i genitori; 3. contatto, nei casi gravi, delle autorità competenti.
Infrazioni: Categoria D	Organo competente e azioni possibili:
Invio di e-mail o messaggi di MSN considerati molestia o bullismo <u>dopo essere stato avvertito</u> . <ul style="list-style-type: none"> • Accedere deliberatamente allo scaricamento o alla diffusione di qualsiasi materiale ritenuto offensivo, osceno, diffamatorio, razzista, omofobico o violento. • Trasmissione di materiale che viola i diritti d'autore di un'altra persona o infranga le condizioni della legge sulla protezione dei dati. Portare il nome della scuola in discredito.	Fare riferimento all'insegnante della classe/ contatto con i genitori Altre possibili azioni di salvaguardia: 1. conservare le prove; 2. informare i provider di servizi di posta elettronica del mittente; 3. fare rapporto alle autorità competenti dove si sospetti la pedofilia o altre attività illegali

MEMBRI MAGGIORENNI DELLA COMUNITÀ SCOLASTICA

(staff, educatori, docenti, personale amministrativo e collaboratori, genitori, studenti ed equiparati)

infrazioni: Categoria A (Cattiva condotta)	Organo competente e azioni possibili:
<ul style="list-style-type: none"> • Uso eccessivo di Internet per attività personali e non in relazione con il proprio profilo e/o sviluppo professionale (es. fare shopping, mail personali, spazi social e messaggeria istantanea e non per uso non professionale ecc.) • Uso di archivi conservazione dati sensibili degli alunni o dei membri della comunità scolastica (es. chiavette USB) senza considerare la possibilità di accesso agli stessi da parte di terzi non autorizzati o senza considerare l'adeguatezza di qualsiasi file memorizzato • Non attuare adeguate procedure di sicurezza/salvaguardia • Qualsiasi comportamento sul World Wide Web che comprometta la professionalità del personale della comunità scolastica. • L'uso improprio dei dati di primo livello di sicurezza, ad esempio l'uso illecito o condivisione di password date a titolo personale • Violazione del copyright o licenza per esempio l'installazione di software senza licenza in rete. 	Si comunica all'amministratore di rete della scuola e al dirigente scolastico che procederà con la somministrazione delle azioni previste dal contratto: <ul style="list-style-type: none"> • avvertimento • ammonizione informale a voce • ammonizione formale scritta
Infrazioni Categoria B (Condotta riprovevole)	Organo competente e azioni possibili:
<ul style="list-style-type: none"> • Abuso grave o danneggiamento intenzionale di qualsiasi hardware computer o software della scuola; 	Denuncia al dirigente scolastico che procederà con la somministrazione delle azioni previste dal contratto:

<ul style="list-style-type: none"> • Qualsiasi tentativo deliberato di violare le norme sulla protezione dei dati o di sicurezza informatica; • La creazione deliberata, l'accesso, il download e la diffusione di qualsiasi materiale ritenuto offensivo osceno, diffamatorio, razzista, omofobico o violento; • Riceve o trasmette materiale che viola le norme del diritto d'autore (copyright) o i diritti di privacy • Lede o diffama il nome della scuola 	<ul style="list-style-type: none"> • avvertimento • ammonizione informale a voce • ammonizione formale scritta • Ulteriori azioni <p>Si attueranno altresì altre azioni di salvaguardia:</p> <ul style="list-style-type: none"> ▪ Riconfigurare i PC in modo sicuro (aumentare la sicurezza delle password o aumentare i filtri di sicurezza) per garantire che non vi è alcun ulteriore accesso inadeguato allo stesso. ▪ Avviare una verifica affidata a ditta esterna specializzata di tutte le attrezzature TIC, come ad esempio i fornitori di servizi gestiti anche direttamente dalla scuola- per garantire che non vi è alcun rischio che di allievi possano accedere a materiali a scuola. ▪ Identificare i dettagli/estremi precisi del "materiale" implicato nell'azione disciplinari <p><u>Quando è il caso: denunciare alla polizia postale o agli organismi legali competenti</u></p>
---	--

Allegato C: procedure operative per la rilevazione, il monitoraggio e la gestione delle segnalazioni e dei casi.

Questa sezione è tratta in parte da **Generazioni Connesse** e condivisa in questa E-Policy in modo da diffondere buone pratiche di rilevazione e segnalazione rilevazione e gestione casi.

La scuola è da sempre il luogo di relazione privilegiato di bambini e adolescenti, l'ambito - insieme alla famiglia - in cui si gioca la grande partita della crescita.

È avamposto privilegiato delle problematiche, dei rischi, dei pericoli che bambini e adolescenti possono vivere ed affrontare ogni giorno.

Pensiamo al bullismo e al cyberbullismo, per esempio, frutto di dinamiche relazionali improntate alla violenza, al non rispetto e all'egoismo che spesso nascono e trovano un primo "sfogo" tra i banchi di scuola. Accorgersi tempestivamente di quanto accade e mettere in atto azioni immediate di contrasto verso questi atti di prepotenza, oltre che di tutela dei ragazzi stessi, diviene fondamentale per poter evitare conseguenze anche a lungo termine che possano pregiudicare il benessere e una crescita armonica dei ragazzi coinvolti.

Riconoscere

La scuola mira ad aiutare a riconoscere il momento in cui ciò che i ragazzi vivono online può essere considerato pericoloso.

Solo conoscendo sarà possibile comprendere in modo approfondito ciascun fenomeno e l'impatto sui ragazzi: ancora troppo spesso gli adulti rischiano di sottovalutare l'effettiva possibilità che i propri alunni (o figli, o bambini e adolescenti conosciuti) possano essersi imbattuti (o avere amici e conoscenti) in quanto descritto.

Si vuole agire per supportare gli insegnanti e il personale scolastico nel riconoscimento e nella costruzione di azioni di contrasto efficaci alle tematiche affrontate.

Potremmo in questo modo:

- aiutare a comprendere che solo un intervento mirato, congiunto e tempestivo può aiutare i bambini, gli adolescenti e le loro famiglie a trovare soluzioni al problema e uno spazio di supporto e di conforto;
- sapere che la helpline di Generazioni Connesse, può essere di aiuto per gestire situazioni problematiche che coinvolgono i più giovani durante la navigazione in Rete;
- conoscere come interviene in questi casi ha l'obiettivo di ricordare che non sei solo/a: c'è una rete di supporto che ti può aiutare.

Generazioni connesse propone due schemi.

- Il primo è la proposta di un "diario di bordo" della scuola nel quale riportare le situazioni problematiche online che vengono affrontate;
- il secondo è una "mappa" che propone alcuni step da seguire per intervenire in modo tempestivo ed efficace qualora si venga a conoscenza di situazioni di pregiudizio che i propri alunni vivono sul web.

Allegato D: documento di e-safety policy consenso dei genitori/tutori per l'accesso ad internet e dichiarazione liberatoria per la pubblicazione di elaborati, nomi, voci, immagini, materiale audiovisivo

I sottoscritti (nome e cognome) _____
a stampatello leggibile

(nome e cognome) _____
a stampatello leggibile

genitori/tutori genitore affidatario dell'alunno/a _____ (NOME E COGNOME)
a stampatello leggibile

iscritto/a alla classe sez. della scuola

'infanzia Primaria secondaria di 1° grado

Di Livorno Ferraris Saluggia

Dichiarano:

- di aver letto e compreso il Documento di E-Safety Policy;
- di essere al corrente che la Scuola mette in atto tutte le precauzioni necessarie per garantire al massimo che gli alunni usino correttamente la rete e non accedano a materiale inadeguato;
- di essere consapevoli che, in considerazione delle precauzioni prese per ridurre al massimo i rischi della navigazione sul WEB, la Scuola non è responsabile di eventuali usi impropri della rete e delle Tecnologie dell'Informazione e della Comunicazione (TIC) né della natura e dei contenuti del materiale che il/la proprio/a figlio/a, aggirando per volontà propria le barriere predisposte dalla scuola, potrebbero reperire in Internet;
- di essere consapevoli della responsabilità individuale del/la proprio/a figlio/a per le eventuali violazioni delle norme e/o per gli eventuali danni provocati da un uso improprio degli strumenti informatici;
- di essere consapevoli che, qualora non venissero rispettate le regole, la scuola adotterà azioni rapportate alla gravità degli episodi e saranno altresì possibili azioni civili per eventuali danni, nonché l'eventuale denuncia all'autorità giudiziaria qualora la violazione si configuri come reato.

Pertanto, i sottoscritti

- acconsentono non acconsentono (*mettere la crocetta su ciò che si vuole fare*) che il/la proprio/a figlio/a utilizzi a scuola l'accesso Internet;
- autorizzano non autorizzano (*mettere la crocetta su ciò che si vuole fare*) l'Istituto Comprensivo "Galileo Ferraris" a realizzare e ad utilizzare, a scopo didattico e/o di documentazione e/o di informazione e senza fini di lucro, fotografie, video o altri materiali audiovisivi contenenti l'immagine, solo il nome, la voce, gli elaborati (scritti, disegni, ...) del proprio/a figlio/a anche, se del caso, mediante riduzioni e/o adattamenti;
- dichiarano di essere informati che detto materiale potrà essere utilizzato per documentare e divulgare le attività della scuola tramite il sito Internet di Istituto, pubblicazioni, cd-rom, mostre, seminari, convegni e altre iniziative promosse dalla scuola anche in collaborazione con altri soggetti legati all'ambito scolastico (es. MIUR, REGIONE o altri enti operanti per conto dello Stato)
- dichiarano di non aver nulla a pretendere in ragione in quanto sopra indicato e di rinunciare irrevocabilmente ad ogni diritto, azione o pretesa derivante da quanto sopra autorizzato.

DATA _____

NOME E COGNOME _____ Firma _____
a stampatello leggibile

NOME E COGNOME _____ Firma _____
a stampatello leggibile

Si allegano fotocopie dei documenti di identità.

Allegato E: documento di e-safety policy assunzione di responsabilità da parte di docenti e altro personale della scuola

Il/La sottoscritto/a, dipendente dell'Istituto
Comprendivo Galileo Ferraris, in qualità di

DICHIARA:

- di aver letto e compreso il Documento di E-Safety Policy;
- di essere consapevole delle responsabilità connesse all'uso delle Tecnologie dell'Informazione e della Comunicazione (TIC) nella scuola.

Pertanto, il/la sottoscritto/a si impegna a:

1. tenere riservate le credenziali di accesso al sistema del registro elettronico o altre piattaforme di studio;
2. modificare la password periodicamente;
3. segnalare tempestivamente eventuali perdite di riservatezza;
4. utilizzare i computer e gli accessi esclusivamente per attività inerenti il proprio servizio e l'aggiornamento professionale;
5. segnalare eventuali anomalie;
6. vigilare sul corretto utilizzo degli strumenti informatici e della navigazione in rete da parte degli alunni.

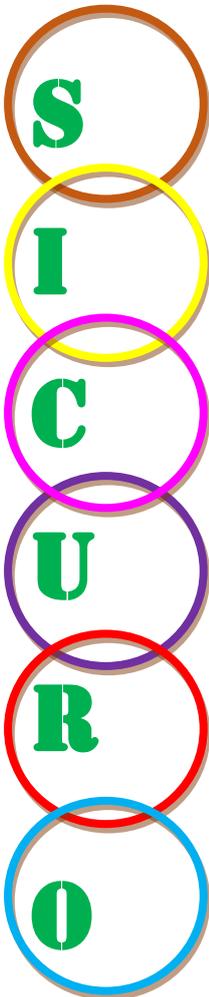
Data _____

Luogo _____

Firma _____

PUA -Corresponsabilità per le diverse età e ruoli.

PRIMA DI CLICCARE PENSA



Se vedo qualcosa che non mi piace sullo schermo, lo dirò sempre ad un adulto

Immagini, video documenti trovati on-line non possono essere sempre usati liberamente

Cliccherò su un'icona o un link solo se sono certo che sono sicuri (me lo ha detto un adulto che conosco bene)

Userò device, internet la mail solo in presenza di un adulto e con il suo permesso

Rispetto prima di tutto! Manderò messaggi scritti con tono rispettoso, propositivo e simpatico. Non scriverò qualcosa che non direi faccia a faccia

Oportunità non un obbligo!
Appena mi è possibile spengo lo strumento che mi tiene connesso e uso la mia testa, gioco imparo e mi diverto stando insieme ad amici e compagni

Data _____
Luogo _____

Firma _____

Allegato F-2: POLITICA DI USO ACCETTABILE DELLA RETE - Per gli alunni dai 9 agli 11 anni

PUA -Corresponsabilità per le diverse età e ruoli.

Questi comportamenti mi aiuteranno a usare in modo sicuro e responsabile strumenti e ambienti online essere rispettoso degli altri e dell'ambiente In cui lavoro: la comunità scolastica

- A scuola userò il computer o i device della scuola, ove non disponibile il cellulare ma solo per motivi didattici (tenuta registro elettronico).
- Mi limiterò a modificare o a cancellare i miei file sui device della scuola.
- Non guarderò, cambierò, cancellerò i file di altre persone senza il loro permesso.
- Terrò le mie password segrete.
- Userò la mail e gli altri strumenti integrati (come lo spazio Google) in modo responsabile e rispettoso degli altri sia nei contenuti scritti che nei contenuti multimediali condivisi.
- Non aprirò o scaricherò file allegati alle mail a meno che non arrivino da persona fidata.
- Non porterò file a scuola senza il permesso dell'insegnante e non condividerò né carico materiali inappropriati per il mio lavoro nello spazio di archiviazione/condivisione (es. Google Drive).
- Sono consapevole del fatto che alcuni siti web e le reti social hanno limiti di età e io devo rispettare queste regole.
- Non tenterò di accedere e visitare siti internet che so essere vietati dalla scuola e non solo.
- Non darò mai il mio indirizzo di casa, numero di telefono cellulare e fisso: non invierò né condividerò fotografie o video e non darò informazioni personali di qualsiasi genere che potrebbero essere utilizzati per identificare me, la mia famiglia o i miei amici: se devo farlo ne parlo prima con un adulto di fiducia.
- Non organizzerò incontri con qualcuno che ho conosciuto su internet, a meno che non abbia il permesso dei miei genitori e vado con loro all'appuntamento.
- se vedo qualcosa online che mi turba, mi spaventa o mi rende infelice o se ricevo un messaggio che mi disturba, non risponderò ma non lo cancellerò: lo farò vedere all'insegnante o a un mio genitore.

Ho letto con attenzione e capito queste regole.

Le accetto da buon cittadino, mi impegno a praticarle dentro e fuori dalla comunità scolastica.

Data _____

Luogo _____

Firma _____

Allegato F-3: POLITICA DI USO ACCETTABILE DELLA RETE- Per gli alunni dagli 11 ai 14 anni

PUA -Corresponsabilità per le diverse età e ruoli.

Questi comportamenti mi aiuteranno a usare in modo sicuro e responsabile strumenti e ambienti on line ed essere rispettoso degli altri e dell'ambiente in cui lavoro: comunità la scolastica.

1. userò solo i computer della scuola, salvo altra indicazione dell'insegnante, e per attività scolastiche e di apprendimento fatte a scuola; sono consapevole che i responsabili della sicurezza on line di istituto possono controllare il mio uso di internet;
2. non porterò file che possono danneggiare la rete della scuola o essere utilizzati per aggirare gli strumenti di sicurezza presenti in istituto;
3. potrò modificare o cancellare solo i miei file e non visualizzare, modificare, cancellare, danneggiare i file di altre persone o di aree di utenti senza il loro permesso (sia online che offline);
4. terrò il mio account di accesso ai servizi della scuola le password segrete, cambiandole regolarmente per evitare gli accessi di persone non autorizzate;
5. userò responsabilmente internet e non andrò a visitare siti web che sono inappropriati per la scuola o per me;
6. spedirò email o contatterò solo persone che conosco o quelle approvate nell'ambito delle attività di apprendimento con il docente referente dell'attività
7. i messaggi che invio o le informazioni che carico saranno sempre rispettose degli altri e dell'ambiente che sto utilizzando: tutti i messaggi che invio infatti parlano della mia reputazione e coinvolgono la reputazione della scuola e della famiglia.
8. farò attenzione quando aprirò i file e gli allegati, quando collegherò memorie esterne; controllerò sempre la presenza di virus e se non sono sicuro non aprirò.
9. non dividerò i miei dati personali che potrebbero essere utilizzati per identificare me, la mia famiglia o i miei amici in qualsiasi spazio online, a meno che un adulto di fiducia mi abbia dato il permesso e controllato la piattaforma che mi richiede i dati.
10. non organizzerò incontri con qualcuno che in precedenza ho sempre e solo incontrato su internet o tramite email o in una chat room, a meno che un adulto di fiducia venga con me.
11. se vedo qualcosa che mi turba, mi spaventa o ricevo un messaggio che mi fa sentire a disagio, non risponderò ad esso; lo salverò e ne parlerò con un adulto di fiducia.
12. sono consapevole del fatto che alcuni siti web, giochi e social network hanno regole rigide sull'età minima di accesso: mi impegno a rispettare questi limiti.
13. sono consapevole che le mie attività online in qualsiasi momento non devono turbare o ferire altre persone e che non dovrebbero mettere a rischio come spesso la mia identità la mia dignità
14. uso di Smart device (smartphone, tablet, notebook) in modalità BYOD (bring your own device)solo quando l'insegnante me lo dirà, potrò portare usare i miei device ma esclusivamente per attività didattiche concordate e se i miei genitori hanno sottoscritto il permesso. Questi strumenti saranno accesi solo quando l'attività lo richiede.
15. mi impegno a non usare i device dei compagni.
16. sono consapevole che la scuola non è responsabile della rottura perdita furto manomissione danneggiamento più o meno grave del mio device, qualsiasi esso sia, in quanto io stesso ne sono responsabile
17. mi impegno a fare registrazioni vocali, foto, video solo se ho un esplicito permesso degli

insegnanti e di altre parti coinvolte (esempio i compagni di classe, i collaboratori, etc.)

18. mi impegno a non divulgare in nessuno spazio online i contenuti condivisi nella cartella della disciplina/corso o sulla piattaforma didattica se non autorizzato.
19. sono consapevole che questa PUA (Policy di utilizzo accettabile) è sintesi della Policy di e-safety di istituto e mi impegno da subito a rispettare e attuare in tutte le sue parti.

Data_____

Luogo_____

Firma_____