UNIONE EUROPEA
FONDI STRUTTURALI EUROPEI
PON 2014-2020
MIUR
Ministero dell'Istruzione, dell'Università e della Ricerca
Dipartimento per la Programmazione
Direzione Generale per interventi in materia di edilizia scolastica, per la gestione dei fondi strutturali per l'istruzione e per l'innovazione digitale
Ufficio IV
PER LA SCUOLA - COMPETENZE E AMBIENTI PER L'APPRENDIMENTO (FSE-FESR)

ISTITUTO COMPRENSIVO G. MICALI
Via degli Archi, 66 57126 Livorno
Tel. 0586/810110
e-mail liic81300x@istruzione.it pec
liic81300x@pec.istruzione.it sito web:
www.icmicalilivorno.gov.it

E-SAFETY POLICY

A.S. 2018-19

A TUTTA LA COMUNITÀ SCOLASTICA
studenti, genitori, docenti e personale ATA

Documento elaborato dalla Commissione composta da:
Dirigente Scolastica, Dott.sa Teresa Cini
Animatore Digitale, Prof. Michele Menicagli
Referente Cyberbullismo dell'IC, Prof. Enrico Pompeo
FS RAV/Invalsi Prof. Pierluigi Maestrini
FS supporto psicopedagogico Prof.ssa Sara Tognazzi
Prof.sse Francesca Ferrara e Giorgia Bacci
Componente studenti classi terze: Jacopo Del Vivo, Cristina Potalivo

Deliberato dal Collegio dei Docenti con delibera n. 11 del 18/02/2019
Deliberato dal Consiglio di Istituto con delibera n. 20 del 04/03/2019

INDICE

1. INTRODUZIONE....1

1.1 Scopo della *Policy*....2
1.2 Ruoli e Responsabilità....3
1.3 Condivisione e comunicazione della Policy all'intera comunità scolastica....7
1.3.1 La condivisione e comunicazione della politica di *e-Safety* agli alunni....7
1.3.2 La condivisione e comunicazione della politica di *e-Safety* al personale....7
1.3.3 La condivisione e comunicazione della politica di *e-Safety* ai genitori....8
1.4 *Gestione delle infrazioni alla Policy*....8
1.4.1 Disciplina degli alunni....9
1.4.2 Disciplina del personale scolastico....9
1.4.3 Disciplina dei genitori....10
1.5 Monitoraggio dell'implementazione della *Policy* e suo aggiornamento....10
1.6 Integrazione della *Policy* con i regolamenti esistenti....11

2. FORMAZIONE E CURRICOLO....12

2.1 Curricolo sulle competenze digitali per gli studenti....12
2.2 Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica....13
2.3 Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali....13
2.4 Sensibilizzazione delle famiglie....14

3. GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE TIC DELLA SCUOLA E DELLA STRUMENTAZIONE PERSONALE....15

3.1 Accesso ad internet....15
3.1.1 Le norme principali....15
3.1.2 Linee guida di buona condotta dell'utente e buone pratiche nell'uso della rete....15
3.2 Gestione accessi....15
3.2.1 Accesso docenti....15
3.2.2 Accesso studenti....16
3.3 E-mail....17
3.4 Sito web della scuola....17
3.5 Social network per alunni docenti e genitori....17
3.6 Registro elettronico....18
3.7 Protezione dei dati personali (GDPR)....18
3.8 Registrazione delle lezioni e strumenti compensativi....19

4. STRUMENTAZIONE DEL PERSONALE.....20

4.1 Per la componente studentesca.....20
4.2 Per la componente personale scolastico (docenti e ATA).....21
4.3 Utilizzo del Laboratorio di Informatica e delle postazioni di lavoro.....21

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI.....23

5.1 Prevenzione.....23
5.2 Rischi e Azioni della scuola rivolte agli studenti e alle loro famiglie.....23
5.3 Sportello di ascolto.....24
5.4 Rilevazione.....25
5.5 Segnalazione.....25
5.5.1 Che cosa segnalare.....25
5.5.2 Come segnalare: procedure operative e strumenti.....25
5.5.3 Gli strumenti per segnalare e monitorare i casi a scuola.....26
5.5.4 Il numero 19.69.6 e servizi di ascolto o segnalazione.....26
5.5.5 Che cosa succede quando segnali?.....27
5.5.6 Procedura per casi gravi di cyberbullismo.....27
5.6 Azioni disciplinari di infrazioni accertate per uso scorretto dello *smartphone*.....28

ALLEGATI

ALLEGATO 1 Modulo per la segnalazione dei casi a cura del docente.....30
ALLEGATO 2 Checklist a cura dei Referenti Sportello di Ascolto.....31
ALLEGATO 3 Schema di procedimento per caso evidente di cyberbullismo.....33
ALLEGATO 4 Modulo di segnalazione al garante per la protezione dei dati personali. 34
ALLEGATO 5 Linee guida per ragazzi di utilizzo di internet.....36
ALLEGATO 6 Linee guida per genitori di utilizzo internet.....37
ALLEGATO 7 Linee guida per la scuola.....39
ALLEGATO 8 Attestato di qualifica “scuola virtuosa".....41

1. INTRODUZIONE

Nell'ambito del progetto "Generazioni connesse" (www.generazioniconnesse.it) cui la scuola ha aderito nel settembre 2017, l'Istituto ha elaborato questo documento programma anche in conformità con le LINEE DI ORIENTAMENTO per azioni di prevenzione e di contrasto al bullismo e cyberbullismo (aprile 2015 e aggiornamento ottobre 2017) elaborate dal MIUR (Ministero dell'Istruzione, dell'Università e della Ricerca) in collaborazione con il *Safer Internet Center* per l'Italia, programma comunitario istituito dal Parlamento Europeo e dal Consiglio dell'Unione Non si tratta di un documento meramente formale, poiché a partire da esso la scuola intende promuovere:

- la formazione rivolta al personale interno circa le tematiche previste dalla *Policy*;
- l'impegno di tutti gli attori coinvolti nel rispetto di quanto definito nel documento;
- l'adeguamento del curricolo per ottemperare a quanto stabilito nella *Policy*;
- la sensibilizzazione dei genitori sul tema della sicurezza online;
- dei partenariati con enti e associazioni esterne.

Internet è un'inestimabile risorsa per l'educazione e l'informazione, offre infinite opportunità per fare ricerca, comunicare, documentare il proprio lavoro, pubblicare elaborati e mettere in comune esperienze. Da un punto di vista amministrativo, grazie all'implementazione costante del sito internet della scuola, all'introduzione del registro elettronico e all'utilizzo della piattaforma web Argo, a cui possono accedere Dirigente, docenti, genitori, alunni e personale amministrativo, è diventato più semplice gestire il sistema-scuola e aprire la scuola all'utenza con una comunicazione più tempestiva, chiara etrasparente.
Allo stesso tempo, l'uso sempre più pervasivo di piattaforme in rete e dispositivi portatili ha esposto gli utenti e in particolare i minori, i soggetti con divario digitale o con limitate competenze informatiche a nuovi rischi, tanto più rilevanti quanto meno è diffusa una cultura relativa ai modi legittimi di usare la rete e alla consapevolezza delle funzioni resepossibili.
L'obiettivo è quello di educare e sensibilizzare gli adolescenti, gli insegnanti e i genitori all'uso sicuro e consapevole di internet.

Definizione di cyber bullismo*: "Bullismo telematico è qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo". (L. 71/2017). A questo si aggiunge che per forma di cyber bullismo la scuola, intende anche la diffusione di contenuti online da parte di alunni con lo scopo di diffamare, denigrare, offendere, alterare, manipolare la persona o l'operato di docenti, personale scolastico, collaboratori ATA, educatori e tutti quelli che fanno parte della formazione ed educazione all'interno del nostro Istituto Comprensivo "G. Micali" di Livorno.*

Pertanto la nostra Scuola ha deciso di sviluppare e attuare il progetto "Generazioni Connesse" (www.generazioniconnesse.it) attraverso la realizzazione di tre linee di intervento:

1. *l'elaborazione di linee guida per una e-Safety Policy d'Istituto, cioè di un proprio codice di condotta nella prevenzione e gestione dei casi di (cyber)bullismo e di un regolamento di sicurezza informatica che ha preso come riferimento i principi proposti dal MIUR nel documento che riassume "La posizione italiana sui principi fondamentali di Internet";*

2. *la cittadinanza digitale con la promozione nei confronti degli alunni della competenza digitale e della cultura del rispetto di regole comuni nell'uso dei servizi telematici e lo sviluppo di regole di buon comportamento (Netiquette) riferite specialmente ai Social Network e della conoscenza delle condizioni del loro utilizzo;*

1.1. Scopo della *Policy*

Lo scopo della *e-Safety Policy* è di condividere e stabilire con tutti i membri della comunità scolastica regole, modalità e principi sull'utilizzo consapevole e corretto di internet.
In particolare essa viene redatta per regolare il comportamento della componente studentesca dentro le aule scolastiche e per sensibilizzarli all'adozione di buone pratiche quando sono fuori dalla scuola. Questo è il caso degli episodi di cyberbullismo, come di altri fenomeni di cui si tratta nella presente politica, che possono avvenire al di fuori della scuola, ma che sono legati alla frequentazione della stessa. Il nostro Istituto accoglie minori "nativi digitali" che fin dalla scuola primaria sono esposti a rischi di cui sono inconsapevoli, pertanto la scuola attua parallelamente attività di prevenzione, controllo e formazione di allieve, allievi e famiglie allo scopo di ridurre al minimo l'occorrenza di atti che non solo creano disagio nella comunità scolastica, ma possono configurarsi come reati.
La scuola opererà, eventualmente, in stretto collegamento con le forze dell'ordine e con le istituzioni del settore educativo, per mettere in campo strategie di prevenzione al cyber-bullismo e interventi di recupero nel caso in cui vengano individuati tali fenomeni, informando i genitori/tutori e chiedendo la loro collaborazione anche qualora gli episodi si siano verificati al di fuori delle attività didattiche.
Le indicazioni, contenute nella presente *e-Safety Policy*, intendono dare al nostro Istituto un impulso allo sviluppo di una cultura d'uso corretto e consapevole di Internet, sia tramite il richiamo a norme vigenti, sia con l'indicazione di prassi e protocolli operativi opportuni per un uso sempre più professionale da parte di tutto il personale e per la prevenzione dei rischi e la gestione delle emergenze.
I principi fondamentali richiamati sono:

- salvaguardare e proteggere i bambini, i ragazzi e tutto il personale dell'Istituto;
- assistere il personale della scuola a lavorare in modo sicuro e responsabile con le tecnologie di comunicazione di Internet e monitorare i propri standard e le proprie prassi didattiche e di comunicazione interna alla scuola;
- impostare chiare aspettative di comportamento e/o codici di condotta rilevanti per un uso responsabile di Internet a scopo didattico, personale o ricreativo;
- adottare un protocollo di intervento per rilevare, monitorare e gestire gli abusi online come il cyerbullismo, che sono riferimenti incrociati con le altre politiche della scuola;
- garantire che tutti i membri della comunità scolastica siano consapevoli del fatto che il comportamento illecito o pericoloso è inaccettabile e che saranno intraprese le opportune azioni disciplinari e giudiziarie.

In particolare l'intento della scuola è quello di promuovere l'uso consapevole e critico da parte degli alunni delle tecnologie digitali e di internet, di far acquisire loro procedure e competenze "tecniche" ma anche corrette norme comportamentali, di prevenire ovvero rilevare e fronteggiare le problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso, delle tecnologie digitali. Gli utenti, siano essi maggiorenni o minori, devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete. Di fatto esiste la possibilità che durante il lavoro online si possa entrare

accidentalmente in contatto con materiale inadeguato e/o illegale, pertanto la Scuola promuove l'adozione di strategie che

limitino l'accesso a siti e/o applicazioni illeciti. In questo contesto, gli insegnanti 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 potenzialmente pericolose. *La presente Policy sarà parte integrante del Regolamento di Istituto, alla sua stesura saranno coinvolti genitori, alunni e tutto il personale della scuola, e portato a conoscenza degli Organi Collegiali e di tutti gli operatori e gli utenti della scuola; con questo atto si intende attivare e mantenere nella nostra scuola una e-Safety Policy in materia di tecnologie dell'informazione e della comunicazione condivisa e accettata da tutti.*

1.2. Ruoli e Responsabilità
(che cosa ci si aspetta da tutti gli attori della Comunità Scolastica)

1. Dirigente scolastico Il ruolo del Dirigente scolastico nel promuovere l'uso consentito delle tecnologie e di internet include i seguenti compiti:	• i dirigenti scolastici sono chiamati a effettuare misure di intervento immediato qualora vengano a conoscenza di episodi di cyber bullismo e dovranno essere integrate e previste nei Regolamenti di Istituto e nei Patti di Corresponsabilità; • Sarà cura del dirigente assicurare la massima informazione alle famiglie di tutte le attività e iniziative intraprese, anche attraverso una sezione dedicata sul sito web della scuola, che potrà rimandare al sito del MIUR www.generazioniconnesse.it; • è auspicabile che il dirigente scolastico attivi specifiche intese con i servizi territoriali (servizi della salute, servizi sociali, forze dell'ordine, servizi minorili dell'amministrazione della Giustizia) in grado di fornire supporto specializzato e continuativo ai minori coinvolti ove la scuola non disponga di adeguate risorse; • garantire 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, un utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della Comunicazione (TIC); • condividere e seguire 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; • a tale scopo necessita di ricevere tempestive informazioni sulle violazioni al presente regolamento o eventuali problemi di cui può venire a conoscenza il corpo docente o il personale ATA;

2. Animatore digitale	• stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornire consulenza e informazioni al personale in relazione ai rischi on-line e alle misure di prevenzione e gestione degli stessi; • si relaziona con la ditta che gestisce l'assistenza tecnico-informatica per definire le misure di sicurezza informatica più opportune • monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, nonché proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola; • assicurare che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate e curarne la manutenzione; • condividere la *e-Safety Policy* sul sito della scuola; • controllo (una tantum e/o all'evenienza di episodi dubbi) del sistema informatico (cronologia, cookies, ecc.) da parte dei responsabili; • installazione di firewall sull'accesso Internet; • aggiornamento periodico del software antivirus e scansione delle macchine in caso di sospetta presenza di virus.

3. DSGA	• assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni; • garantire il funzionamento dei diversi canali di comunicazione della scuola (sportello, circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet.
4. Referente per il cyber/bullismo	• il docente referente potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav); • il referente ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio; • assicurare che l'educazione alla sicurezza online sia incorporata in tutto il programma di studi; • promuovere la consapevolezza e l'impegno per la salvaguardia online in tutta la comunità scolastica; • promuovere la formazione e dare consulenza a tutto il personale; • promuovere attività o progetti da svolgere nelle classi; • applicare e controllare i protocolli di rilevazione, monitoraggio e gestione delle potenziali azioni di cyber bullismo; • diffusione della *e-Safety Policy* attraverso power point e schede semplificative; • collaborare con tutte le agenzie educative e istituzionali (associazioni sportive, polizia postale, associazioni di sostegno, etc.) per prevenire e gestire i casi di possibile cyber bullismo; • coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti l'utilizzo consapevole di internet.
5. Il personale scolastico (ATA, segreterie, etc)	• essere consapevoli dei problemi di sicurezza on-line connessi con l'uso di telefoni cellulari, fotocamere e dispositivi portatili; • comprendere e contribuire a promuovere politiche di sicurezza on line; • monitorare l'uso di dispositivi tecnologici e attuare politiche scolastiche per quanto riguarda questi dispositivi; • segnalare qualsiasi abuso, anche sospetto, o problema alla Dirigente e ai responsabili della sicurezza online; • usare comportamenti sicuri, responsabili e professionali nell'uso della tecnologia: le comunicazioni digitali con gli studenti devono avvenire esclusivamente a livello professionale e solo attraverso i sistemi scolastici, non attraverso meccanismi personali, per esempio e-mail, telefoni cellulari, ecc.

6. I Docenti Il ruolo del personale docente e di ogni figura educativa che lo affianca include i seguenti compiti:	• aver letto, compreso e sottoscritto la presente *Policy*; • informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento; • studio e nelle attività didattiche ed educative delle classi; • assicurare che gli alunni abbiano una buona comprensione delle opportunità e dei rischi di ricerca offerte dalle tecnologie digitali; • garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali limitando a casi particolari le comunicazioni digitali private; • evitare partecipazione a gruppi di condivisione di *whatsapp* o altro, inerenti la scuola (gruppi classe, gruppi genitori, etc..), se non autorizzati dalla Dirigente; • assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente; • segnalare al Dirigente scolastico, al vicario del Dirigente scolastico e al referente sul bullismo, evidenze di abusi rilevati a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dai protocolli qui adottati; • gli insegnanti sono responsabili delle TIC nell'ambito dell'attività didattica e hanno il compito di responsabilizzare gli alunni per divenire consapevoli dell'importanza della salvaguardia di un bene comune, seguendo le corrette norme di utilizzo; • controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito); • nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei specificandone la fonte di provenienza; • comunicare al referente sul bullismo e alla Dirigente scolastica, bisogni o disagi espressi dagli alunni durante l'utilizzo di Internet, della piattaforma o di altre TIC, da parte dei ragazzi; • attenzione all'utilizzo di penne USB, CD/DVD o altri dispositivi esterni personali e dell'istituto; • dare chiare indicazioni sul corretto utilizzo della rete (Internet, piattaforma studenti ecc.), condividendo con gli alunni la netiquette e indicandone le regole; • non divulgare le credenziali di accesso agli account (username e password) e/o, nel caso ne sia a conoscenza, alla rete wifi; • non allontanarsi dalla postazione lasciandola incustodita, se non prima di aver effettuato la disconnessione; • non salvare sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili; • proporre agli alunni attività di ricerca di informazioni in rete fornendo opportunamente loro indirizzi dei siti e/o parole chiave per la ricerca cui fare riferimento. • illustrare ai propri alunni le regole di utilizzo contenute nel presente documento; • aver letto, compreso e sottoscritto la presente *Policy*; • sensibilizzare i genitori ad una lettura attenta e condivisa con i propri figli del presente documento.

7. Gli Alunni	• essere responsabili, in relazione al proprio grado di maturità e di apprendimento, per l'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti; • avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali ma anche della necessità di evitare il plagio e rispettare i diritti d'autore; • comprendere l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi; • adottare condotte rispettose degli altri anche quando si comunica in rete; • esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori. • leggere, comprendere, ed accettare la *e-Safety Policy* • capire l'importanza di segnalare abusi, o l'uso improprio o l'accesso a materiali inappropriati; • sapere quali azioni intraprendere se loro o qualcuno che conoscono si sente preoccupato o vulnerabile quando si utilizza la tecnologia on-line; • conoscere e capire la politica relativa all'uso dei telefoni cellulari, fotocamere digitali dispositivi portatili; • conoscere e capire la politica della scuola sull'uso di immagini e il cyberbullismo; • capire l'importanza di adottare buone pratiche di sicurezza on-line quando si usano le tecnologie digitali fuori dalla scuola; • assumersi la responsabilità di conoscere i benefici e i rischi di utilizzo di Internet e di altre tecnologie in modo sicuro, sia a scuola che a casa; • non utilizzare propri dispositivi esterni personali senza aver acquisito il permesso da parte dell'insegnante; • chiudere correttamente la propria sessione di lavoro. • utilizzare le TIC , SOLO, su indicazioni del docente; • accedere all'ambiente di lavoro con il corretto account (per gli alunni delle classi per le quali è stato attivato un account *google apps for education*), non divulgandone le credenziali di accesso (username, password), e archiviare i propri documenti in maniera ordinata e facilmente rintracciabile nella cartella di ogni LIM riferiti alla classe in cui è presente; • non manomettere le impostazioni dei PC della scuola.
8. I Genitori	• Sostenere e condividere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle tecnologie dell'Informazione e delle Comunicazioni nella didattica; • Seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllare l'utilizzo del PC e di internet; • Concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di internet; • Fissare delle regole per l'utilizzo del computer e tenere sotto controllo l'uso che i figli fanno di internet e del telefonino in generale; • sostenere la scuola nel promuovere la sicurezza online e approvare la e-*Policy*; • utilizzare gruppi di condivisione su ***whatsapp*** **all'interno delle classi per comunicazioni inerenti la scuola, utilizzando un linguaggio appropriato e nel rispetto di tutti**

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

L'Istituto si impegna a diffondere la presente *Policy* per condividerne i contenuti con tutta la comunità scolastica.
La *Policy* sarà comunicata al personale, agli alunni, alla comunità nei seguenti modi:

- pubblicazione della *e-Safety Policy* sul sito della scuola nel menù a sinistra;
- accordo di utilizzo accettabile, discusso con gli studenti e i genitori, all'inizio del primo anno, tramite il **Patto di Corresponsabilità**, che sarà sottoscritto dalle famiglie e rilasciato alle stesse;
- accordo di utilizzo accettabile rilasciato al personale scolastico.

Successivamente si condividerà nelle seguenti modalità a seconda degli attori interessati per raggiungere in modo più incisivo le singole parti:

1.3.1. La condivisione e comunicazione della politica di e-Safety agli alunni

- attraverso la discussione in classe della *Policy* nei primi giorni di scuola, con particolare riguardo al protocollo di utilizzo di internet per le nuove classi prime;
- attraverso l'inserimento dell'indice tematico di questo documento nel libretto scolastico e in particolare dei comportamenti da attuare in caso di bisogno.
- istruire e informare gli alunni riguardo all'uso responsabile e sicuro di internet precederà l'accesso alla rete;
- dare comunicazione dell'elenco delle regole per la sicurezza on-line che sarà pubblicato in tutte le aule o laboratori con accesso a internet;
- a tal proposito si manterrà l'attivazione di uno "Sportello di ascolto" rivolto a tutti gli alunni, articolato in colloqui individuali e/o collettivi, al fine di migliorare il benessere personale e scolastico mediante un'attività di supporto della sfera emotiva, relazionale e comportamentale. Si prevede al suo interno, anche uno spazio riservato ai docenti e genitori al fine di individuare strategie efficaci per affrontare problematiche tipiche dell'età adolescenziale.

1.3.2. La condivisione e comunicazione della politica di e-Safety al personale

- la linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet sarà discussa negli organi collegiali (Consigli di Interclasse, Collegio dei Docenti) e comunicata formalmente a tutto il personale con il presente documento e altro materiale informativo anche sul sito web;
- per proteggere tutto il personale e gli alunni, la scuola metterà in atto una linea di condotta di utilizzo accettabile, controllato e limitato alle esigenze didattiche informazione/formazione on-line del personale docente nell'uso sicuro e responsabile di internet, sia professionalmente che personalmente, sarà fornita a tutto il personale, anche attraverso il sito web della scuola;
- il sistema di filtraggio adottato e il monitoraggio sull'utilizzo delle TIC sarà supervisionato dall'Animatore digitale, che segnalerà al DSGA eventuali problemi che dovessero richiedere acquisti o interventi di tecnici;
- tutto il personale è consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile.
- un confronto collegiale, su base annuale, circa la necessità di apportare modifiche e miglioramenti alla *Policy* vigente, in una fase successiva la Commissione E-*Policy* provvederà alle relative modifiche;

- elaborazione di protocolli condivisi di intervento.

1.3.3. La condivisione e comunicazione della politica di e-Safety ai genitori

- l'attenzione dei genitori sulla sicurezza nell'uso delle tecnologie digitali e di internet sarà attirata nelle news o in altre aree del sito web della scuola;
- sarà incoraggiato un approccio di collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di internet in occasione degli incontri scuola-famiglia, assembleari, collegiali e individuali;
- la scuola fornirà ai genitori suggerimenti e indicazioni per l'uso sicuro delle tecnologie digitali e di internet anche a casa;
- i docenti di classe forniranno ai genitori indirizzi sul web relativi a risorse utili per lo studio e a siti idonei per gli alunni funzionalmente alle attività didattiche progettate;
- l'organizzazione di incontri di sensibilizzazione sul tema della sicurezza informatica e di informazione circa i comportamenti da monitorare o da evitare.
- allo scopo di condividere regole comuni per l'utilizzo sicuro di Internet sia a casa che a scuola, si invitano tutti i genitori a prestare la massima attenzione ai principi e alle regole contenute nel presente documento. Si richiede che ogni genitore e/o tutore si impegni a farle rispettare ai propri figli anche in ambito domestico, primariamente assistendo i minori nel momento dell'utilizzo della rete e poi ponendo in atto tutti i sistemi di sicurezza che aiutino a diminuire il rischio di imbattersi in materiale indesiderato.

1.4. Gestione delle infrazioni alla *Policy*

Le infrazioni alla *Policy* possono essere rilevate da docenti/ATA nell'esercizio delle proprie funzioni oppure possono essere segnalate da alunni e genitori a docenti/ATA, referente cyberbullismo, vicario della Dirigente e al Dirigente scolastico stesso. Qualora esse si configurino come vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso. Il Dirigente scolastico ha la facoltà di revocare l'accessibilità temporanea o permanente ai laboratori informatici e/o all'utilizzo di strumenti tecnologici (PC, tablet, notebook, ecc) a chi non si attiene alle regole stabilite. La scuola prenderà tutte le precauzioni necessarie per garantire la sicurezza on-line. Tuttavia, a causa della scala internazionale collegata ai contenuti Internet, la disponibilità di tecnologie mobili e velocità di cambiamento, non è possibile garantire che il materiale non idoneo apparirà mai su un computer della scuola o dispositivo mobile. Né la scuola né l'autorità locale possono accettare la responsabilità per il materiale accessibile, o le conseguenze di accesso a Internet. Al personale e agli alunni saranno date informazioni sulle infrazioni in uso e le eventuali sanzioni contenute nel Regolamento di Istituto o nel presente documento. Nel caso in cui le infrazioni della *Policy* violino norme previste dal Regolamento di Istituto si procede secondo quanto previsto dal Regolamento stesso; qualora le infrazioni riguardino l'opportunità di certi comportamenti o la convivenza civile, la scuola eroga delle sanzioni secondo il principio della sensibilizzazione e del risarcimento dell'eventuale danno provocato, in uno spirito di recupero e rieducazione.
Nelle sezioni successive al presente documento sono, inoltre, richiamate e specificate le infrazioni e relative sanzioni.

I provvedimenti includono:

- qualsiasi rilevamento di sospetto abuso, offesa, procurato disagio ricevuto su internet, sia personale che di un compagno, sarà sempre riferito, da parte del personale scolastico, al Dirigente Scolastico e al referente del bullismo che fungeranno da primo punto di contatto;

- possibile ritiro del cellulare fino a fine giornata;

- saranno informati e documentati i genitori o i tutori per condividere con loro le strategie più opportune;
- denunce di bullismo online saranno trattate in conformità con la legge attuale. Reclami relativi alla protezione dei bambini saranno trattati in conformità alle procedure di protezione dell'infanzia;
- successivamente, nei casi più gravi, saranno avviate le comunicazioni alle autorità competenti;
- qualora esse si configurino come vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso. Infatti è bene ricordare a tutti 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.

1.4.1. Disciplina degli alunni

Le potenziali infrazioni in cui è possibile che gli alunni incorrano a scuola nell'utilizzo delle tecnologie digitali di internet di cui si dispone per la didattica, in relazione alla fascia di età considerate, sono prevedibilmente le seguenti:

- un uso della rete per giudicare, infastidire o impedire, in modo persistente, a qualcuno di esprimersi o partecipare;
- l'invio incauto o senza permesso di foto o di altri dati personali come l'indirizzo di casa o il telefono;
- l'invio o la condivisione di immagini intime o troppo spinte;
- il collegamento a siti web, nell'orario scolastico, non autorizzati dai docenti;
- l'utilizzo, non autorizzato o comunicato ai docenti, dello *smartphone* in orario scolastico (utilizzando messaggeria, video , audio o foto). Gli interventi correttivi previsti per gli alunni sono rapportati all'età e al livello di sviluppo dell'alunno.

Infatti più gli alunni sono piccoli, più i comportamenti "da correggere" sono dovuti a uno sviluppo cognitivo, affettivo e morale incompleto o a fasi critiche transitorie, che devono essere compresi e orientati proprio dagli educatori, nella prospettiva del raggiungimento di una maggiore consapevolezza e maturità da parte dell'alunno.
Sono previsti pertanto da parte dei docenti **provvedimenti "disciplinari" proporzionati all'età e alla gravità del comportamento.**
Contestualmente sono previsti interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi dei disagi causati, di ri-definizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli alunni della classe, di prevenzione e gestione positiva dei conflitti, di moderazione dell'eccessiva competitività, di promozione di rapporti amicali e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni.

1.4.2. Disciplina del personale scolastico

Le potenziali infrazioni in cui è possibile che il personale scolastico e in particolare i docenti incorrano nell'utilizzo delle tecnologie digitali e di internet sono diverse e alcune possono determinare, favorire o avere conseguenze di maggiore o minore rilievo sull'uso corretto e responsabile delle TIC da parte degli alunni:

- un utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di insegnamento o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei;
- un utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;

- un trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- una diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- una carente istruzione preventiva degli alunni sull'utilizzazione corretta e responsabile delle tecnologie digitali e di internet;
- una vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili incidenti;
- insufficienti interventi nelle situazioni critiche di contrasto a terzi, correttivi o di sostegno agli alunni, di segnalazione ai genitori, al Dirigente scolastico, all'Animatore digitale.

Il Dirigente scolastico può controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a internet, la posta elettronica inviata/pervenuta a scuola, procedere alla cancellazione di materiali inadeguati o non autorizzati dal sistema informatico della scuola, conservandone una copia per eventuali successive investigazioni. Tutto il personale è tenuto a collaborare con il Dirigente scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio di 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.

1.4.3. Disciplina dei genitori

In considerazione dell'età degli alunni e della loro dipendenza dagli adulti, anche alcune condizioni e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola, dove possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico.
Le situazioni familiari meno favorevoli sono:

- la convinzione che se il proprio figlio rimane a casa ad usare il computer è al sicuro e non combinerà guai;
- una posizione del computer in una stanza o in un posto non visibile a tutti quando è utilizzato dal proprio figlio;
- una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'utilizzo del cellulare o dello *smartphone* senza una periodica condivisione o controllo dei contenuti;
- la mancanza di adeguata conoscenza che la responsabilità dei contenuti dello *smartphone*
  dei minori è sempre ascrivibile ai genitori/tutori;
- assoluto disinteresse sui contenuti dello *smartphone* dei propri figli;

I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli, se dovessero risultare pericolosi per sé e/o dannosi per gli altri.

1.5. Monitoraggio dell'implementazione della *Policy* e suo aggiornamento

Le regole relative all'accesso ad Internet vengono approvate dal Collegio dei Docenti e dal Consiglio di Istituto e pubblicate sul sito della scuola. Gli alunni vengono informati del fatto che l'utilizzo di Internet è monitorato e vengono date loro istruzioni per un uso responsabile e sicuro. Il personale scolastico riceve una copia del Regolamento, che viene

sottoscritta e osservata scrupolosamente. Tutto il personale scolastico, pertanto, è coinvolto nel monitoraggio dell'utilizzo di Internet, nello sviluppo delle linee guida e nell'applicazione delle

istruzioni sull'uso sicuro e responsabile di Internet. Il monitoraggio dell'implementazione della *Policy* e del suo eventuale aggiornamento sarà svolta ogni anno. Tale monitoraggio sarà curato dal Dirigente scolastico con la collaborazione dell'Animatore digitale, dal referente del cyber bullismo e dai docenti delle classi, tramite questionari e conversazioni. Sarà finalizzato a rilevare la situazione iniziale delle classi e gli esiti a fine anno, in relazione all'uso sicuro e responsabile delle tecnologie digitali e di internet. Il monitoraggio sarà rivolto anche agli insegnanti, al fine di valutare l'impatto della *Policy* e la necessità di eventuali miglioramenti. L'aggiornamento della *Policy* sarà curato dal Dirigente Scolastico, dal referente cyber bullismo e dagli Organi Collegiali, a seconda degli aspetti considerati. La *e-Safety Policy* si inserisce all'interno di altre politiche scolastiche, quali la politica di protezione dei minori, la politica anti-bullismo, la politica del benessere degli alunni a scuola Come già ricordato, la *e-Safety Policy* sarà riesaminata annualmente o quando si verificano cambiamenti significativi per quanto riguarda le tecnologie in uso all'interno della scuola e tutte le modifiche della *Policy* saranno discusse in dettaglio con tutti i membri del personale docente.

Nell'ambito del monitoraggio dell'implementazione della *e-Safety Policy* si terranno in considerazione i dati annuali sulla base del seguente documento che verrà aggiornato in corso d'anno e pubblicato in via definitiva a chiusura dell'attività didattica:

ANNO SCOLASTICO	NUMERO di segnalazioni	NUMERO di infrazioni	NUMERO di sanzioni disciplinari
2018/19	n. 1	n. 1	/ /

1.6. Integrazione della *Policy* con i regolamenti esistenti

La presente *e-Safety Policy* o regolamento per l'uso delle risorse tecnologiche e di rete è stato allegato al Regolamento di Istituto e inserito nel sito web della scuola.
I genitori vengono informati della pubblicazione del presente "Regolamento per l'uso delle risorse tecnologiche e di rete" della scuola e possono prenderne visione sul sito della scuola.

2. FORMAZIONE E CURRICOLO

Il nostro Istituto condivide le linee indicate nel Piano Nazionale Scuola Digitale (PNSD). Esse danno come indirizzo l'intento di modificare gli ambienti di apprendimento per rendere l'offerta formativa coerente con i cambiamenti della società della conoscenza e con le esigenze e gli stili cognitivi delle nuove generazioni.
Si ricorda il D.M. 851 del 27 ottobre 2015, in attuazione dell'art.1, comma 56 della legge 107/2015, che ne prevede l'attuazione al fine di:

- migliorare le competenze digitali degli studenti anche attraverso un uso consapevole delle stesse;
- implementare le dotazioni tecnologiche della scuola al fine di migliorare gli strumenti didattici e laboratoriali ivi presenti;
- favorire la formazione dei docenti sull'uso delle nuove tecnologie ai fini dell'innovazione didattica;
- individuare un Animatore Digitale ed un team per l'innovazione digitale che supporti ed accompagni adeguatamente l'innovazione didattica, nonché l'attività dell'animatore Digitale;
- partecipare a bandi nazionali ed europei per finanziare le suddette iniziative;

2.1. Curricolo sulle competenze digitali per gli studenti

Le Nuove Indicazioni Nazionale del 2012, in raccordo con il programma europeo Competenze chiave, prevedono che al termine del primo ciclo di istruzione lo studente possegga buone competenze digitali e sappia usare con consapevolezza le tecnologie della comunicazione per ricercare e analizzare dati ed informazioni, per distinguere informazioni attendibili da quelle che necessitano di approfondimento, di controllo e di verifica e per interagire con soggetti diversi nel mondo. In questo senso le TIC (Tecnologie dell'Informazione e della Comunicazione) preparano gli studenti ad un'attiva e consapevole partecipazione ad un mondo in rapida evoluzione e nel quale è necessario acquisire abilità e competenze in grado di facilitare l'adattamento dell'individuo ai continui cambiamenti. Si rende quindi necessario lo sviluppo e la diffusione di una mentalità tecnologica diffusa e precoce, intesa come alfabetizzazione al senso, all'utilizzabilità in contesti dati e per scopi definiti da un lato; ed acquisizione sempre più consapevole di strategie efficaci per il dominio di una macchina complessa che impiega e genera oggetti immateriali, dall'altro. Gli alunni dovrebbero 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. Le TIC possono infatti offrire significative occasioni per sviluppare le competenze di comunicazione, collaborazione e *problem-solving*.
Nell'ambito del PNSD questa scuola si propone un programma di progressiva educazione alla sicurezza online come parte del curriculum scolastico. Si impegna a sviluppare una serie di competenze e comportamenti adeguati alle età degli alunni e ad esperienza, tra cui:

- programmare attività e far partecipare gli alunni a laboratori di utilizzo consapevole e appropriato delle TIC;
- capire il comportamento accettabile quando si utilizza un ambiente online, vale a dire, essere educato, non utilizzare comportamenti inappropriati, mantenere le informazioni personali private;

- conoscere le conseguenze disciplinari della scuola, civili e penali in caso di denuncia e riscontro oggettivo di infrazioni inerente un utilizzo scorretto degli *smartphone* e contrario alla presente *Policy* o al regolamento di istituto;
- capire il motivo per cui non devono pubblicare foto o video di altri senza il loro permesso;
- capire il motivo per cui qualsiasi materiale scritto, pubblicato e postato sui social è sempre tracciabile e può rimanere per sempre;
- capire che condividere è essere ugualmente responsabili di ciò che vi è all'interno del gruppo;
- capire perché "amici" on-line potrebbero non essere chi dicono di essere e di comprendere perché dovrebbero fare attenzione in un ambiente online;
- capire il motivo per cui non dovrebbero inviare o condividere resoconti dettagliati delle loro vite personali e informazioni di contatto;
- comprendere l'impatto di bullismo online, *sexting*, *grooming* e sapere come cercare aiuto se sono in pericolo;
- sapere come segnalare eventuali abusi tra cui il bullismo on line e come a chiedere aiuto ai docenti, ai genitori, se si verificano problemi quando si utilizzano le tecnologie Internet;
- utilizzare con attenzione Internet per garantire che si adatti alla loro età e supporti gli obiettivi di apprendimento per le aree curriculari specifiche;
- sviluppare una serie di strategie per valutare e verificare le informazioni prima di accettarne l'esattezza;
- essere a conoscenza che l'autore di un sito web/pagina può avere un particolare pregiudizio;
- sapere come restringere o affinare una ricerca.

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

La formazione del corpo docente verrà organizzata su due livelli: interno ed esterno. A livello interno, nel PTOF si prevede che una parte della formazione in servizio sia dedicata proprio all'uso e all'inserimento delle TIC nella didattica e ai temi informatici in generale. Tale formazione è svolta o da docenti dell'Istituto con formazione specifica o organizzando incontri tenuti da esperti esterni per permettere una adeguata formazione agli insegnanti stessi.
Per quanto riguarda la formazione esterna, la scuola assicura tempestiva e capillare informazione su corsi, convegni e seminari che riguardino tali argomenti, cercando altresì di agevolare il personale che intenda parteciparvi. Infine la scuola può aderire alla formazione di rete di Ambito 11 che prevede un modulo formativo sulla competenza digitale, livello base e avanzato. Ne scaturisce il ruolo fondamentale che deve assumere la Comunità scolastica nel guidare gli studenti verso la consapevolezza dei propri diritti e doveri di "cittadini virtuali".

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

La formazione in ingresso e in servizio è senza dubbio il cardine per assicurare l'adeguatezza della professionalità docente ai bisogni formativi ed educativi degli studenti. Prioritario, infatti, appare il coinvolgimento degli insegnanti ai quali vanno rivolti moduli

di formazione che rafforzino le competenze necessarie a individuare tempestivamente eventuali risvolti psicologici conseguenti all'uso distorto delle nuove tecnologie e alla violenza in contesti faccia a faccia. La scuola partecipa dal 2017/18 al programma "generazioni connesse" sui cui è

disponibile una piattaforma di formazione destinata a tutti i docenti dell'Istituto che vogliano formarsi sull'argomento specifico delle nuove tecnologie.
Nel corso dell'a.s. 2018/19 è stato organizzato un incontro con le figure istituzionali dell'Ufficio Minori e con la Polizia Postale per far fronte alla richiesta da parte della comunità scolastica di avere maggiore informazione e formazione possibile, visto anche il continuo progredire di applicazioni o siti social utilizzati dai ragazzi.

2.4.Sensibilizzazione delle famiglie

La scuola avrà continua cura di sensibilizzare le famiglie attraverso documentazione informativa ed incontri ad un corretto uso delle nuove tecnologie da parte dei ragazzi a casa e a scuola, indicando anche alcune semplici azioni che possono rendere la navigazione sicura.
In modo particolare:

- far conoscere, condividere e presentare ai genitori il Regolamento della *Policy*, al fine di garantire che i principi di comportamento sicuro on-line siano chiari;
- promuovere la partecipazione dei genitori stessi alla discussione e revisione periodica della presente *Policy*;
- offrire incontri di consulenza con esperti;
- fornire informazioni sui siti nazionali di sostegno per i genitori, quali il sito www.generazioniconnesse.it.

3. GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE TIC DELLA SCUOLA E DELLA STRUMENTAZIONE PERSONALE

La scuola metterà in atto tutte le azioni necessarie per garantire agli studenti l'accesso alla documentazione cercata adottando tutti i sistemi di sicurezza conosciuti per diminuire le possibilità di rischio durante la navigazione. Resta fermo che non è possibile garantire una navigazione totalmente priva di rischi e che la Scuola e gli insegnanti non possono assumersi le responsabilità conseguenti all'accesso accidentale e/o improprio a siti illeciti.

3.1. Accesso a internet

Il nostro Istituto ha configurato un proxy server per monitorare il traffico web e per bloccare l'accesso a siti inappropriati a un contesto scolastico.
Occorre, inoltre, sensibilizzare tutta la comunità scolastica sull'opportunità di mantenere aggiornati gli antivirus installati sulle macchine personali e controllare i dispositivi di archiviazione esterna che vengano collegati al proprio PC.

3.1.1. Le norme principali

1. l'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante;
2. internet non può essere usato per scopi vietati dalla legislazione vigente;
   l'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet;
3. è vietato inserire sui PC connessi in rete programmi contenenti virus, scaricare software non autorizzati da internet, scaricare e installare software senza licenza.

Consultare obbligatoriamente prima di installare qualsiasi programma l'animatore digitale, un responsabile di laboratorio o un tecnico per valutarne la compatibilità.

3.1.2. Linee guida di buona condotta dell'utente e buone pratiche nell'uso della rete

- rispettare la legislazione vigente;
- tutelare la propria privacy, quella degli altri utenti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni elettroniche cui hai accesso;
- rispettare la cosiddetta *netiquett*e (regole condivise che disciplinano il rapportarsi fra utenti della rete, siti, forum, mail e di qualsiasi altro tipo di comunicazione);
- controllo della validità e dell'origine delle informazioni a cui si accede o che si ricevono;
- utilizzo di fonti alternative di informazione per proposte comparate;
- ricerca del nome dell'autore, dell'ultimo aggiornamento del materiale e di altri possibili link al sito;
- rispetto dei diritti di autore e dei diritti di proprietà intellettuale.

3.2. Gestione accessi

3.2.1. Accesso docenti

L'Istituto attualmente è dotato di una rete wireless destinata all'utilizzo didattico da parte

del corpo docente.

La password è unica a livello di Istituto/plesso. Ai docenti è consentito accedere ad Internet dai propri dispositivi utilizzando la rete Wi-Fi dell'Istituto previa richiesta alla Dirigente o al suo vicario. La scuola sta valutando, per tracciare gli utilizzi fatti della rete, la possibilità di abbinare l'ID del proprio PC ad accessi autorizzati registrando indirizzo rete di ogni PC e la sua corrispondente attività. Ciascun utente connesso alla rete dovrà rispettare il presente regolamento e la legislazione vigente succitata, 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 e rispettare la cosiddetta *netiquette* (insieme di regole, comunemente accettate e seguite da quanti utilizzano Internet e i servizi di rete, che disciplinano il comportamento di un utente nel rapportarsi agli altri utenti attraverso risorse come *wiki*, *newsgroup*, *mailing list*, *forum*, *blog* o e-mail).
La componente studentesca dovrà impegnarsi a rispettare le norme di buon utilizzo che la scuola ha elencato nel presente documento.
Ogni docente è tenuto ad un controllo della strumentazione in aula (PC e portatili) poiché l'uso del dispositivo è permesso agli alunni solo su autorizzazione dell'insegnante. Ogni docente accede al registro elettronico attraverso una password che non può essere comunicata a terzi, né agli alunni.
Per quanto riguarda la connessione a internet, si ricorda che:

- l'accesso può avvenire unicamente da tale dispositivo;
- il proprietario del dispositivo è l'unico responsabile di tutte le operazioni svolte con esso;
- in caso di furto o smarrimento del dispositivo identificato si deve immediatamente informare il personale tecnico incaricato che ne revocherà l'accesso alla rete;
- il docente dell'ultima ora verificherà lo spegnimento della postazione al termine lezioni;

3.2.2. Accesso studenti

Il Regolamento di Istituto vieta l'uso del cellulare.
In particolare, agli studenti non è consentito accedere ad Internet da propri dispositivi utilizzando la rete wi-fi dell'Istituto. Durante l'orario scolastico agli alunni non è permesso l'utilizzo della telefonia mobile; è altresì vietato l'uso per scopo personale di tutti gli altri strumenti informatici di proprietà e non dello studente. L'eventuale utilizzo di strumenti informatici di proprietà dello studente durante l'attività didattica deve essere autorizzata dal docente. In riferimento alla **C.M. del 15 Marzo 2007** nella quale si precisa che "Laddove se ne ravvisi l'opportunità, il regolamento di istituto potrà prevedere le misure organizzative più idonee atte a prevenire, durante le attività didattiche, il verificarsi del fenomeno di un utilizzo scorretto del telefonino", questo documento, parte integrante del Regolamento di Istituto, norma la possibilità per i docenti (in accordo con le famiglie) di raccogliere gli *smartphone* in un contenitore comune da porre sulla cattedra e, nel caso di attività in palestra, portare detto contenitore nella palestra stessa al fine di non lasciare i dispositivi incustoditi nell'aula vuota. In caso contrario, nel corso delle lezioni, **i cellulari devono rimanere di norma spenti nello zaino di ogni studentessa/studente.**
Relativamente agli alunni che accedono a Internet durante l'attività didattica sono consentiti la navigazione guidata da parte dell'insegnante e la stesura di documenti collaborativi purché sotto il controllo dell'insegnante e nel caso in cui tale attività faccia parte di un progetto di lavoro precedentemente autorizzato. È vietato l'accesso alle chat-room pubbliche o non moderate.
La trasgressione di queste regole provocherà una sanzione decisa dal Dirigente e dal CdC secondo le presenti norme e in accordo al Regolamento di Istituto.

3.3. E-mail

Solo i docenti possono utilizzare i servizi mail accedendo alla rete della scuola a fini esclusivamente didattici. Sulla rete scolastica tutti sono invitati a utilizzare solo account di posta elettronica facilmente identificabili (@istruzione.it) e per scopi inerenti lo svolgimento didattico/organizzativo.
Le comunicazioni tra personale scolastico, famiglie e allieve/allievi via e-mail devono avvenire preferibilmente tramite un indirizzo e-mail della scuola o all'interno della piattaforma di apprendimento tramite registro elettronico (@istruzione.it), per consentire l'attivazione di protocolli di controllo.
E-mail in arrivo da mittenti sconosciuti vanno trattate come sospette ed eventuali allegati non devono essere aperti.

3.4.Sito web della scuola

Il Dirigente Scolastico e il personale incaricato di gestire le pagine del sito della Scuola hanno la responsabilità di garantire che il contenuto pubblicato sia accurato e appropriato. La scuola offre all'interno del proprio sito una serie di servizi alle famiglie e ai fruitori esterni: i docenti che desiderano pubblicare attività didattiche dovranno chiedere l'autorizzazione al Dirigente.

3.5.*Social network* per alunni, docenti e genitori.

Per la Legge l'utilizzo dei *Social Network* con la pubblicazione di nomi e giudizi sulle persone o sulle istituzioni e la diffusione di foto/filmati senza il consenso e, comunque, all'insaputa delle persone coinvolte può determinare ricadute di carattere anche penale, come ad esempio la diffamazione.

Si invitano pertanto tutti gli studenti a non prelevare o diffondere immagini, video o registrazioni - anche solo audio - non autorizzate, ed eliminare da internet eventuali riferimenti offensivi o comunque illeciti (ed inopportuni) nei confronti dell'Istituto e dei suoi docenti e studenti.

Allo stesso tempo, si invitano gli allievi e i genitori a fare un uso prudente dei *Social Network*, in particolare *facebook* e *whatsapp*, limitandone l'uso alle sole comunicazioni funzionali, evitando ad ogni modo di esprimere giudizi sull'operato degli altri studenti o del personale della scuola, giudizi che una volta pubblicati comportano sempre una assunzione di responsabilità da parte di chi li ha scritti o anche semplicemente diffusi. Nella pratica didattica si cercherà di educare la componente studentesca al loro uso sicuro. L'IC, al fine di realizzare la campagna di raccolta di finanziamenti per l'attivazione di un nuovo laboratorio digitale linguistico ha creato la propria pagina *facebook* che comparirà nella vetrina del portale *School Raising* e nella quale saranno caricate foto descrittive degli eventi realizzati nella scuola.

3.6. Registro elettronico

Ogni famiglia riceve le credenziali per l'accesso riservato al registro elettronico, in cui il corpo docente è tenuto a registrare assenze, valutazioni, note e osservazioni. L'uso del registro elettronico verrà spiegato alle famiglie nel corso di un incontro orientativo che si terrà alle famiglie all'apertura dell'anno scolastico oltre che ad alcune indicazioni guida da pubblicarsi sul sito della scuola. La pubblicazione delle informazioni attraverso tale strumento assolve l'obbligo di comunicare prontamente ed efficacemente ogni evento riguardante l'alunno/a. Coloro che non possono accedere a Internet e di conseguenza non possono consultare il registro elettronico sono pregati di darne segnalazione al coordinatore del consiglio di classe, che verificherà la trascrizione delle comunicazioni sul diario e la firma dei genitori.

3.7. Protezione dei dati personali (GDPR)

Il 25 maggio 2018 è entrato in vigore in tutti gli stati aderenti all'Unione Europea il Regolamento del Parlamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, conosciuto come GDPR (General Data Protection Regulation).
Anche se in parte quanto previsto dal nuovo Regolamento risulta facilmente sovrapponibile alla precedente normativa italiana, è però necessario ricordare che il GDPR diventa il nuovo riferimento per garantire la corretta tutela dei dati personali. Pertanto il nostro Istituto adeguerà le modalità e responsabilità opportune a questo documento.
Garantire la corretta tutela dei dati personali richiede, innanzitutto, l'individuazione dei dati trattati soggetti alla normativa vigente, nonché l'analisi delle modalità e responsabilità di gestione delle informazioni, onde identificare le eventuali criticità e gli adeguamenti da predisporre.
Saranno da individuare le misure di tutela attuate e da definire quelle da attuare, nonché le modalità per garantirne nel tempo la continuità e l'adeguatezza.
Dovranno inoltre essere stabilite le responsabilità per la gestione dei dati: titolare, responsabile, persone autorizzate al trattamento. L'Istituto Comprensivo "G. Micali" di Livorno ha stipulato in rete un contratto annuale con la nuova figura del RPD, nella persona dell'Ing. A. Bove, Ditta Oxfirm. La raccolta ed il trattamento di dati personali avvengono, quando necessari, in relazione all'esecuzione di
servizi richiesti dall'utente, o quando l'utente stesso decide di comunicare i propri dati personali; in tali circostanze, la presente politica della privacy illustra le modalità ed i caratteri di raccolta e trattamento dei dati personali dell'utente. L'I.C. tratta i dati personali forniti dagli utenti in conformità alla normativa vigente.
Tuttavia, si possono individuare al riguardo alcune linee guida di *e-Safety*: "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.

Si deve quindi prestare particolare attenzione prima di caricare immagini e video su blog o social network, oppure di diffonderle attraverso mms o sistemi di messaggistica istantanea. Succede spesso, tra l'altro, che una fotografia inviata a un amico o a un familiare venga poi inoltrata ad altri destinatari, generando involontariamente una comunicazione a catena dei dati personali raccolti. Tale pratica può dar luogo a gravi violazioni del diritto alla

riservatezza delle persone riprese, e fare incorrere in sanzioni disciplinari, pecuniarie e in eventuali reati

(da vademecum privacy del Garante). L'utilizzo di telefoni cellulari, di apparecchi per la registrazione di suoni e immagini, quando autorizzato dai docenti, è consentito, ma esclusivamente per fini personali, e sempre nel rispetto dei diritti e delle libertà fondamentali delle persone coinvolte (siano essi studenti o professori) in particolare della loro immagine e dignità. Le istituzioni scolastiche hanno, comunque, la possibilità di regolare o di inibire l'utilizzo di registratori, *smartphone*, tablet e altri dispositivi elettronici all'interno delle aule o nelle scuole stesse. Gli studenti e gli altri membri della comunità scolastica, in ogni caso, non possono diffondere o comunicare sistematicamente i dati di altre persone (ad esempio pubblicandoli su Internet) senza averle prima informate adeguatamente e averne ottenuto l'esplicito consenso (da vademecum privacy del Garante).

3.8. Registrazione delle lezioni e strumenti compensativi

È possibile registrare la lezione esclusivamente per scopi personali, ad esempio per motivi di studio individuale. Per ogni altro utilizzo o eventuale diffusione, anche su Internet, è necessario prima informare adeguatamente le persone coinvolte nella registrazione (professori, studenti…) e ottenere il loro esplicito consenso. Nell'ambito dell'autonomia scolastica, gli istituti possono decidere di regolamentare diversamente o anche di inibire l'utilizzo di apparecchi in grado di registrare. In ogni caso deve essere sempre garantito il diritto degli studenti con diagnosi DSA (disturbi specifici dell'apprendimento) o altre specifiche patologie di utilizzare tutti gli strumenti compensativi (come il registratore) di volta in volta previsti nei piani didattici personalizzati che li riguardano (da vademecum privacy del Garante):

- è consigliabile utilizzare canali istituzionali per comunicazioni a scopo didattico con le famiglie e gli studenti;
- come e-mail si utilizzerà quella istituzionale della scuola (liic81300x@istruzione.it) per avere tracciabilità della conversazione in un luogo protetto;
- le fotografie o i video da pubblicare sul sito che includano allieve e allievi saranno selezionati con cura e non permetteranno a singoli di essere chiaramente identificati a meno che non si tratti di eventi particolari per cui le famiglie potranno concedere opportuna autorizzazione. La scuola cercherà di utilizzare fotografie o video di gruppo piuttosto che foto integrali di singoli;
- i nomi completi di alunne e alunni saranno evitati sul sito web come pure nei blog, forum e wiki, in particolare se in associazione con le loro fotografie;
- all'atto dell'iscrizione è richiesto alle famiglie di firmare un'autorizzazione scritta per consentire l'uso didattico di immagini e video delle/dei minori secondo i principi sopra indicati;
- ogni caso particolare sarà preso in considerazione per stabilire l'opportunità di pubblicare dati personali e sarà presentata apposita richiesta circostanziata che varrà solo per lo specifico evento.

4. STRUMENTAZIONE DEL PERSONALE
durante l'orario scolastico

4.1. Per la componente studentesca

Gli studenti non possono utilizzare i propri dispositivi durante le attività didattiche come previsto dal regolamento di istituto, né possono accedere alla rete attraverso i dispositivi della scuola se non con autorizzazione dell'insegnante presente in aula e comunque per ricerche attinenti le attività didattiche. Studenti con disturbi specifici di apprendimento o altre disabilità certificate, previa consultazione con il Consiglio di Classe, concorderanno le modalità di impiego di strumenti compensativi quali tablet e computer portatili e le modalità di custodia nell'armadietto della classe.
Nel caso in cui debbano comunicare con la famiglia durante l'orario scolastico, alunne e alunni possono usare gratuitamente la linea fissa della scuola rivolgendosi a un operatore; allo stesso modo le famiglie devono chiamare il centralino della scuola se hanno assoluta necessità di parlare con i propri figli. Si raccomanda di ridurre tali comunicazioni a casi di inderogabile necessità e urgenza.
L'invio di materiali abusivi, offensivi o inappropriati è vietato, anche se avviene all'interno di cerchie o gruppi di discussione privati.
Salvo casi del tutto eccezionali, i telefoni cellulari non devono essere portati a scuola e non devono comunque essere utilizzati durante l'orario scolastico. Se, malgrado il divieto appena espresso, gli studenti verranno sorpresi ad usare il cellulare, verrà chiesto dal docente di porlo temporaneamente nel cassetto della cattedra, che verrà chiuso a chiave fino al termine delle lezioni dai docenti e poi restituito alla famiglia convocata o, in mancanza di questa, al ragazzo stesso. Verrà immediatamente comunicato l'accaduto al referente del cyberbullismo, alla Dirigente e al suo primo collaboratore. Si convocheranno per vie brevi i genitori interessati ai quali verrà, possibilmente, riconsegnato il cellulare.
Considerando il fatto che gli *smartphone* possono essere utilizzati anche per scattare foto o effettuare riprese, si informano i Sigg. genitori che eventi di questo tipo, se concretizzati durante l'orario scolastico, si possono configurare anche come reati per i quali non si esclude la segnalazione ai competenti organi di Pubblica Sicurezza.

In particolare, a riguardo di un uso scorretto dello *smartphone*, si ricorda che:
a. La scuola non pone alcun ostacolo all'utilizzo di cd/dvd rom o di hard disk portatili come strumenti di lavoro e di studio. Ciò che a riguardo compete alle famiglie è il controllo periodico del contenuto di questi strumenti per evitare che qualche studente "trasporti" a scuola immagini, testi o filmati per così dire "sconvenienti", scaricati dalla rete o da terzi.
b. Per impedire che le stesse postazioni dei laboratori scolastici possano essere furtivamente utilizzate per visitare siti volgari e pericolosi, la scuola si è da tempo dotata di un software di sicurezza che filtra gli accessi ad internet e protegge quindi i visitatori meno esperti. Oltre a questo sofisticato sistema di protezione che blocca l'accesso ai siti di cui si discorre, la scuola ovviamente mette in campo soprattutto la vigile attenzione educativa di ogni singolo docente.
c. Fermo restando il fatto che la scuola è un'istituzione educativa e che non è prevista, né possibile, né tantomeno legittima, la perquisizione quotidiana di tutti gli studenti all'inizio di ogni giorno di lezione, le responsabilità che dovessero derivare dal verificarsi di eventi riconducibili all'uso non corretto o non legittimo di uno qualsiasi degli oggetti

di cui alla presente norma regolamentare sono tutte ascrivibili alle famiglie degli studenti eventualmente coinvolti.

d. Le responsabilità appena menzionate sono condivise dal personale scolastico solo quando e solo se, avendo personalmente constatato o essendo venuto a conoscenza che qualche ragazzo/a fa uso di un device (*smartphone* o tablet) durante l'orario scolastico e lo utilizza in modo scorretto e contro il regolamento di istituto non dovesse immediatamente intervenire nelle forme già indicate e comunque in modo tale da prevenire o reprimere sul nascere situazioni incompatibili con le più elementari regole della civile convivenza.

4.2. Per la componente personale scolastico (docenti e ATA)

I docenti possono utilizzare i dispositivi della scuola per realizzare tutte le attività connesse alla funzione docente. È consentito per i docenti l'uso dei propri dispositivi in classe per quanto attiene l'attività didattica qualora siano necessari, ma non possono essere utilizzati durante le lezioni per questioni personali. Il personale preferirà, quando ciò è possibile, l'impiego della strumentazione fornita dalla scuola rispetto a quella personale (portatili, PC fissi, ecc.); le infrastrutture e gli apparati della scuola non vanno utilizzati per scopi personali. Telefoni cellulari, tablet, fotocamere e altri strumenti di registrazione audio/video non devono essere impiegati durante le lezioni scolastiche se non all'interno di attività didattiche programmate. L'uso improprio della rete è contestato al titolare delle credenziali con cui è avvenuta la comunicazione.
Qualora si utilizzino a scuola dispositivi di archiviazione esterna di proprietà personale (chiavette usb, dischi fissi portatili) è bene controllare preventivamente che essi siano esenti da virus per evitare di danneggiare le attrezzature comuni.
Durante l'attività didattica è opportuno che ogni insegnante:

- dia chiare indicazioni sul corretto utilizzo della rete (Internet, piattaforma studenti ecc.), condividendo con gli studenti la *netiquette* e indicandone le regole;
- si assuma la responsabilità di segnalare prontamente eventuali malfunzionamenti o danneggiamenti al tecnico informatico;
- non salvi sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili e proponga agli alunni attività di ricerca di informazioni in rete fornendo opportunamente loro indirizzi dei siti e/o parole chiave per la ricerca cui fare riferimento.

4.3. Utilizzo del Laboratorio di Informatica e delle postazioni di lavoro

Disposizioni sull'uso del laboratorio

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. quando un insegnante, da solo o in classe, usufruisce del laboratorio deve obbligatoriamente registrare il proprio nome e l'eventuale classe nell'apposito registro delle presenze di laboratorio, indicando l'orario di ingresso, quello di uscita e motivazione dell'uso delle postazioni informatiche; questo allo scopo di poter risalire alle cause di eventuali inconvenienti o danneggiamenti e per comprovare l'effettivo utilizzo dell'aula;

4. l'ingresso degli allievi nei laboratori è consentito solo in presenza dell'insegnante;
5. il docente accompagnatore è responsabile del corretto uso didattico di hardware e software;
6. nei laboratori è vietato utilizzare CD personali o altri dispositivi se non dopo opportuno controllo con sistema di antivirus aggiornato;
7. è vietato cancellare o alterare files e dati presenti sull'hard disk;
8. è vietato alterare le impostazioni del PC, di rete o altro;
9. il laboratorio non deve mai essere lasciato aperto o incustodito quando nessuno lo utilizza; all'uscita dal laboratorio sarà cura di chi lo ha utilizzato lasciare il mobilio in ordine, le macchine spente correttamente;
10. in caso di malfunzionamento o guasto dei computer bisogna darne tempestiva segnalazione al responsabile del laboratorio;
11. in caso di malfunzionamento non risolvibile dal responsabile di laboratorio si contatterà personalmente o attraverso il Responsabile di laboratorio, la segreteria;
12. per motivi di manutenzione straordinaria, in caso di guasti o di virus, i PC possono essere formattati senza preavviso; Si consiglia pertanto di salvare i dati importanti su CD o pen drive periodicamente; In caso di formattazione ordinaria ci sarà un preavviso;
13. all'uscita dal laboratorio sarà cura di chi lo ha utilizzato lasciare il locale in ordine e le macchine spente correttamente;
14. l'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante;
15. il Responsabile di laboratorio che verifichi un uso del laboratorio contrario a disposizioni di legge o del regolamento interno deve darne comunicazione per iscritto al Dirigente Scolastico.

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

5.1. Prevenzione

Come scuola intendiamo per prevenzione un insieme molto ampio di strategie che coinvolgano le famiglie e le forze sociali che operano sul territorio al fine di mettere al proprio centro l'educazione formativa dei ragazzi. Contrastare il bullismo implica la creazione di una comunità solidale, in cui ogni allievo accetta sia il diritto di vivere una scuola senza violenza, sia la responsabilità di difendere i compagni più vulnerabili. Il coinvolgimento dei coetanei è indispensabile per creare un clima di solidarietà, combattere l'omertà e l'indifferenza, incoraggiare le vittime a chiedere aiuto, sottrarre al bullo i potenziali proseliti.
Nello specifico, la scuola, attiverà una serie di misure:

- integrare nel curricolo temi legati al corretto utilizzo delle TIC e di Internet;
- **progettare UdA specifiche che verranno pianificate a livello di dipartimenti disciplinari, garantendo un intervento su ogni classe, anche con docenti non titolari della classe;**
- supportare e implementare la competenza digitale in tutti i ragazzi all'interno delle materie curricolari.

Si demanda ai settori disciplinari la scelta dei settori su cui focalizzare la formazione. La scuola si avvale, inoltre, della collaborazione di enti e associazioni per realizzare incontri rivolti alla componente studentesca e alle famiglie con l'intento di fornire ogni elemento utile alla prevenzione e alla gestione dei problemi relativi alla sicurezza informatica; le famiglie sono invitate a proporre tematiche di particolare interesse su cui la scuola focalizzerà il proprio intervento.
L'Istituto comprensivo attiva inoltre uno sportello di ascolto al quale la componente studentesca si può rivolgere per avere consigli e sostegno psicologico anche relativamente alle tematiche del cyber- bullismo.

5.2. Rischi e Azioni della scuola rivolte agli studenti e alle loro famiglie

Il nostro istituto integra l'offerta formativa con attività finalizzate alla prevenzione e al contrasto del bullismo e del cyberbullismo, nell'ambito delle tematiche afferenti a Cittadinanza e Costituzione per tradurre i "saperi" in comportamenti consapevoli e corretti, indispensabili a consentire alle giovani generazioni di esercitare la democrazia nel rispetto della diversità e delle regole della convivenza civile. Le indicazioni relative ad un utilizzo sicuro della Rete da parte degli studenti potranno essere oggetto di specifici moduli didattici, da inserire nel Piano dell'Offerta Formativa (POF).
La strategia di contrasto dei fenomeni del bullismo dovrebbe essere costituita, quindi, già a partire dalle scuole primarie, da un insieme di misure di prevenzione rivolte agli studenti di varia tipologia.
Tra le specifiche azioni da programmare si possono prevedere le seguenti, anche sulla base della attività svolte nell'a.s. 2017/18:

1. coinvolgimento di tutte le componenti della comunità scolastica nella prevenzione e nel contrasto del bullismo e del cyberbullismo, favorendo la collaborazione attiva dei genitori;
2. attività laboratoriali specifiche sul tema da svolgere in classe;
3. integrazione della presente *Policy* con il Regolamento di Istituto;

4. comunicazione agli studenti e alle loro famiglie sulle sanzioni previste dal Regolamento di Istituto nei casi di bullismo, cyberbullismo e navigazione online a rischio;
5. somministrazione di questionari agli studenti e ai genitori finalizzati al monitoraggio, anche attraverso questionari online con pubblicazione dei risultati sul sito web della scuola, che possano fornire una fotografia della situazione e consentire una valutazione oggettiva dell'efficacia degli **interventi attuati (v. Progetto "Senza Rischio" in rete di Ambito**);
6. percorsi di formazione tenuti da esperti rivolti ai genitori sulle problematiche del bullismo e del cyberbullismo impostati anche sulla base dell'analisi dei bisogni;
7. mantenimento dell'apertura di uno Sportello di ascolto;
8. utilizzo di procedure codificate per segnalare alle famiglie e/o organismi competenti i comportamenti a rischio.

RISCHI	AZIONI
Adescamento online (*grooming*)	Sensibilizzazione sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni e per indurli alla prostituzione. Qualora si venga a conoscenza di casi simili, occorre valutarne la fondatezza e avvisare il Dirigente Scolastico per l'intervento delle forze dell'ordine.
Cyberbullismo	Campagne di sensibilizzazione e informazione anche con l'ausilio di progetti e realtà esterni. I casi possono essere molto variegati, variando dal semplice scherzo di cattivo gusto via sms/*whatsapp* a vere e proprie minacce verbali e fisiche, che costituiscono reato. Occorre confrontarsi con il Dirigente Scolastico sulle azioni da intraprendere.
Dipendenza da Internet, videogiochi, shopping o *gambling online*, …	Informazioni sul fatto che ciò può rappresentare una vera e propria patologia che compromette la salute e le relazioni sociali e che in taluni casi (per es. uso della carta di credito a insaputa di altri) rappresenta un vero e proprio illecito.
Violazione della privacy	Informazione sull'esistenza di leggi in materia di tutela dei dati personali e di organismi per farle rispettare. Se il comportamento rilevato viola solo le norme di buona convivenza civile e di opportunità, occorre convocare i soggetti interessati per informarli e discutere dell'accaduto e concordare forme costruttive ed educative di riparazione. Qualora il comportamento rappresenti un vero e proprio illecito, il Dirigente Scolastico deve esserne informato in quanto sono previste sanzioni amministrative o penali.

È fondamentale, perciò, far comprendere la nozione basilare secondo cui la propria ed altrui sicurezza in Rete non dipende solo dalla tecnologia adottata (software anti-virus, anti- malware, apparati vari etc.) ma dalla capacità di discernimento delle singole persone nel proprio relazionarsi attraverso la Rete.

5.3. Sportello di ascolto

Tra le misure di prevenzione che la scuola mette in atto ci sono, altresì, azioni finalizzate a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze così che

l'utilizzo di Internet e dei cellulari oltre che collocarci all'interno di un sistema di relazioni, ci renda consapevoli di gestire con un certo grado di lucidità i rapporti che si sviluppano in tale ambiente, giungendo a riconoscere e gestire le proprie emozioni. A tal proposito è attivo uno "Sportello di ascolto" nella persona di una psicologa reclutata da bando dedicato, rivolto all'intero personale scolastico al fine di migliorare il benessere personale e scolastico mediante un'attività di supporto della sfera emotiva, relazionale e comportamentale e anche al fine di individuare strategie efficaci per affrontare problematiche tipiche dell'età adolescenziale. Lo Sportello è attivo anche in ogni plesso dell'IC nelle persone di docenti counselor.

5.4. Rilevazione

La rilevazione dei casi è compito dell'intera comunità educante, secondo la sensibilità di ciascuno e la presenza in particolari momenti o contesti. A partire dalla corretta formazione e sensibilizzazione, **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.*** Accorgersi tempestivamente di quanto accade e compiere azioni immediate di contrasto verso gli atti inopportuni - quando non illegali - diviene fondamentale per poter evitare conseguenze a lungo termine che possano pregiudicare il benessere e una crescita armonica dei soggetti coinvolti.

5.5. Segnalazione

5.5.1. Che cosa segnalare Intervenire: sì o no? SEMPRE.

Siamo chiamati a garantire il benessere dei nostri alunni, oltre che a trasmettere conoscenze. Se un alunno ha confidato qualcosa che lo preoccupa di ciò che accade online, significa che si fida di noi e pensa che si abbiano le risorse per aiutarlo.

5.5.2. Come segnalare: procedure operative e strumenti

PROCEDURE OPERATIVE IN CASO DI SOSPETTO O EVIDENTE EPISODIO DI CYBERBULLISMO

1	**Ascolta**: chiedigli/le cosa puoi fare per lui/lei e cosa desidera che accada.
2	**Se l'alunno ci porge spontaneamente le prove i docenti possono consultarle e condividerle con lui.**
3	**Avvisare e comunicare immediatamente l'accaduto al Dirigente scolastico**, al vicario e al referente cyberbullismo.
4	**Avere un colloquio con la "vittima" o accogliere la sua segnalazione** alla presenza di chi ha rilevato il caso, del referente del cyberbullismo e della Dirigente Scolastica (o vicario).
5	Assicurarsi **che l'alunno vittima salvi nel suo telefono ogni messaggio,** voce/testo/immagine, conservando così il numero del mittente.
6	**Avvisare telefonicamente i genitori** della vittima che conservi e condivida il contenuto e fare in modo che la famiglia si accerti della segnalazione ricevuta. Fare in modo che la famiglia si accerti della segnalazione.

7	**Conservare la prova, per il genitore, è utile** per far conoscere l'accaduto in base alla gravità ai genitori degli alunni bulli, al Dirigente scolastico e per le condotte criminose alla polizia.

8	Qualora non si disponga di prove, ma solo delle testimonianze dell'alunno, quantunque riferite a fatti accaduti al di fuori del contesto scolastico, le notizie raccolte sono comunque comunicate ai genitori e per fatti rilevanti anche al Dirigente scolastico; per quelle criminose, anche alla polizia.
9	**Accertarsi del danno** e avere copia o *screenshot* della conversazione dal genitore della vittima.
10	**Intervenire con il protocollo di intervento (ALLEGATO 3**): agire per ridare benessere al/la tuo/a alunno/a.
11	**Avere un colloquio con il "bullo" o i "bulli",** alla presenza di chi ha rilevato il caso, del referente del cyberbullismo e della Dirigente Scolastica (o vicario).
12	**Chiamare per un colloquio i genitori del "bullo" o dei "bulli",** per condividere la gravità della situazione rilevata e comunicare le successive azioni da mettere in atto
13	In base all'urgenza le comunicazioni formali possono essere precedute da quelle informali, effettuate per le vie brevi.
14	**Fermare immediatamente l'abuso.**
15	**Consultare il numero 1.96.96,** soprattutto nei casi gravi o complessi.
16	**Convocare il consiglio di classe** che nel caso sia necessario applichi eventuali sanzioni.
17	**Applicare la sanzione** comunicandolo ai genitori.
18	**Avvisare in casi gravi la Polizia Postale e delle Comunicazioni.**

5.5.3. Gli strumenti per segnalare e monitorare i casi a scuola

Di seguito sono reperibili due strumenti che potranno agevolare la segnalazione.
Nell'effettuare la segnalazione seguire ed utilizzare il **Modulo per la segnalazione dei casi a cura del docente (ALLEGATO 1),** affinché le segnalazioni vengano effettuate per iscritto e contengano tutte le informazioni necessarie alla presa in carico della situazione, e il **Modulo di segnalazione al garante per la protezione dei dati personali** (**ALLEGATO 4**).
Come già detto per la prevenzione, il coinvolgimento dei coetanei è indispensabile per garantire l'efficacia dell'intervento ed è finalizzato a:

- creare un clima di solidarietà;
- combattere l'indifferenza e la deresponsabilizzazione morale;
- incoraggiare le vittime a chiedere aiuto;
- sottrarre al (cyber)bullo potenziali proseliti.

5.5.4. Il numero 1.96.96. e servizi di ascolto o segnalazione

La *linea di ascolto* ***1.96.96*** **(**attiva 24 ore su 24 per 365 giorni all'anno) e la *chat* **(**attiva tutti i giorni dalle 8.00 alle 22.00 (sabato e domenica dalle 8.00 alle 20.00) di **Telefono Azzurro** accolgono qualsiasi richiesta di ascolto e di aiuto da parte di bambini/e e ragazzi/ e fino ai 18 anni o di adulti che intendono confrontarsi su situazioni di disagio/pericolo in cui si trova un minorenne. Il servizio di *help-line* è riservato, gratuito e sicuro, dedicato ai giovani o ai loro familiari che possono chattare, inviare e-mail o parlare al telefono con professionisti qualificati relativamente a dubbi, domande o problemi legati all'uso delle nuove tecnologie digitali e alla sicurezza online.

Inoltre, è disponibile l'applicazione ***youpol*** che si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima.
I due servizi messi a disposizione dal *Safer Internet Center* sono:

- **Clicca e segnala** di *Telefono Azzurro* **www.azzurro.it/it/clicca-e-segnala**
- **Stop-it** di *Save the Children* **www.stop-it.it**.

È importante fornire solo le informazioni che si hanno a disposizione e non attivarsi per ricercarne altre: in questo caso si rientrerebbe nella ricerca proattiva di materiale pedopornografico e di conseguenza passibili di reato.
Avvisare in casi gravi la **Polizia Postale e delle Comunicazioni,** attualmente impegnata in diverse attività a sostegno della navigazione protetta dei minori, competente a ricevere segnalazioni su qualsiasi tipo di reato informatico.

5.5.5. Che succede quando segnali?

Sulla base della segnalazione ricevuta, gli operatori di entrambi i Servizi (YOUPOL E TELEFONO AZZURRO) procedono a coinvolgere le Autorità competenti per la gestione degli interventi più opportuni a fronte del contenuto o della piattaforma segnalata. È bene specificare però che, trattandosi di materiali spesso illegali, all'utente non è richiesto di cercare più informazioni rispetto a quelle che già possiede al momento della segnalazione.
Per questo la nostra Scuola opererà una politica di intervento sia **reattiva** che **pro-attiva.**
Quella **reattiva** dovrà prevedere azioni di supporto al (cyber)bullo perché compia un processo di maturazione che lo porti a comprendere che qualsiasi forma di sopraffazione non è accettabile. Quella **proattiva**, richiede la partecipazione di tutte le componenti della comunità scolastica e dovrà essere rivolta a insegnare a tutti, potenziali bulli e vittime, sia come essere assertivi, sia come saper gestire la propria aggressività e istinto di sopraffazione, promuovendo un'interazione tra pari più responsabile. Le procedure interne per la rilevazione e la gestione dei casi, nonché la segnalazione alla Dirigenza Scolastica ed eventualmente alle autorità competenti, avvengono secondo i protocolli suggeriti dalla piattaforma messa a disposizione da "Generazioni Connesse", come da schemi allegati.

5.5.6. Procedura per gravi casi di cyberbullismo

In riferimento alla legge 71/2017 nel caso in cui un minore sia oggetto di **atti di cyberbullismo gravi, pesanti e reiterati nel tempo**, è prevista la richiesta di oscuramento, rimozione o blocco di qualsiasi dato personale del minore medesimo.
La richiesta è effettuata dal minore che abbia compiuto i quattordici anni o (per i minori di 14 anni) dal genitore o dall'esercente la responsabilità genitoriale e va inoltrata:

- al titolare del trattamento
- al gestore del sito internet
- al gestore del social media

Se i soggetti responsabili non comunicano di aver preso in carico la segnalazione entro 24 ore dal ricevimento della stessa, l'interessato può rivolgersi, mediante segnalazione o reclamo, al Garante per la protezione dei dati personali.
Il Garante provvede entro quarantotto ore dal ricevimento della richiesta.
Altre modalità di segnalazione riguardano quelle, effettuate dalle scuole, di episodi di cyberbullismo e materiale pedopornografico on line.
I primi (episodi di cyberbullismo) vanno segnalati al servizio *Helpline* di Telefono Azzurro 1.96.96, una piattaforma integrata che si avvale di telefono, chat, sms, *whatsapp* e *skype*.
Tali strumenti, leggiamo nelle Linee di Orientamento, sono adeguati ad aiutare i ragazzi e le ragazze a comunicare il proprio disagio.

5.6. Azioni disciplinari di infrazioni accertate per uso scorretto dello *smartphone*

<table>
<tr><th colspan="3">INFRAZIONE</th><th>SANZIONE DISCIPLINARE</th></tr>
<tr><td rowspan="5">FUORIDALL'ORARIOSCOLASTICO</td><td rowspan="4">Tra compagni di classe</td><td>Diffusione di foto o video non autorizzate, tra compagni di classe fuori orario scolastico. È compreso il divieto alla condivisione su gruppi.</td><td rowspan="5">• Richiamo scritto riportato sul Registro di classe;
• Comunicazione formale alla famiglia;
• Comunicazione formale al Dirigente dei ripetuti richiami scritti sul Registro ed alla famiglia.
• Deferimento al Consiglio di Classe/Interclasse (delle classi parallele del plesso coinvolto) quali organi collegiali preposti alle sanzioni sino a 15 giorni.</td></tr>
<tr><td>Offese e insulti tramite messaggi di testo, e-mail, pubblicati su social network (whatsapp, instagram, facebook, etc…) tra compagni di classe fuori orario scolastico. Compresa anche la condivisione e diffusione.</td></tr>
<tr><td>Diffusione di foto o video che ritraggono situazioni intime, violente o spiacevoli tramite il cellulare, siti web o social network, tra compagni di classe fuori orario scolastico, compresa la condivisione su gruppi.</td></tr>
<tr><td>Furto, appropriazione, uso e rivelazione ad altri di informazioni personali come le credenziali d'accesso all'account e-mail, social network, tra compagni di classe fuori orario scolastico.</td></tr>
<tr><td rowspan="2">Al personale scolastico</td><td>Offese e insulti tramite messaggi di testo, e-mail, pubblicati su social network (whatsapp, instagram, facebook, etc…) sul personale scolastico fuori orario scolastico. Compresa la sua diffusione e condivisione su gruppi.</td></tr>
<tr><td>Diffusione di foto o video non autorizzate in cui sia presente personale scolastico fuori dall'orario scolastico È compreso anche il divieto alla condivisione su gruppi.</td></tr>
<tr><td rowspan="4">INTERNO ALL'ORARIO SCOLASTICO</td><td rowspan="2">Tra compagni di classe</td><td>Offese e insulti tramite messaggi di testo, e-mail, pubblicati su social network (whatsapp, instagram, facebook, etc…) a compagni all'interno dell'orario scolastico e nei locali della scuola, compreso la sua condivisione e diffusione su gruppi.</td><td rowspan="4">POSSIBILI SANZIONI
• Richiamo scritto riportato sul Registro di classe;
• Comunicazione formale alla famiglia;
• Comunicazione formale al Dirigente
• Deferimento al Consiglio di Classe/Interclasse quali organi collegiali preposti alle sanzioni fino a 15 giorni.
• Deferimento al consiglio d'Istituto per violazioni disciplinari di estrema gravità: per ripetuti e gravi atti di bullismo o cyberbullismo accertati e avvenuti all'interno della scuola</td></tr>
<tr><td>Diffusione di foto o video non autorizzate a compagni all'interno dell'orario scolastico e nei locali della scuola. È compreso anche il divieto alla condivisione su gruppi.</td></tr>
<tr><td rowspan="2">Al personale scolastico</td><td>Offese e insulti tramite messaggi di testo, e-mail, pubblicati su social network (whatsapp, instagram, facebook, etc…) a personale scolastico all'interno dell'orario scolastico e nei locali della scuola.
Sono comprese anche condivisione e diffusione</td></tr>
<tr><td>Diffusione di foto o video non autorizzate del personale scolastico all'interno dell'orario scolastico e nei locali della scuola.
È compreso anche il divieto alla condivisione su gruppi.</td></tr>
</table>

ALLEGATO 1 - MODULO PER LA SEGNALAZIONE DEI CASI A CURA DEL DOCENTE

Descrizione dell'episodio o del problema		
Soggetti coinvolti	Vittima/e: 1. _____ 2. _____ _____ Bullo/i: 1. _____ 2. _____ 3. _____	Classe: _____ _____ _____ Classe: _____ _____ _____
Chi ha riferito dell'episodio ?	☐ La vittima ☐ Un compagno della vittima, nome: _____ ☐ Genitore, nome: _____ ☐ Insegnante, nome: _____ ☐ Altri, specificare: _____	
Atteggiamento del gruppo	Da quanti compagni è sostenuto il bullo? _____ Quanti supportano la vittima o potrebbero farlo? _____	
Gli insegnanti sono intervenuti in qualche modo?	_____ _____ _____	
La famiglia o altri adulti hanno cercato di intervenire?	_____ _____ _____	
Chi è stato informato della situazione?	☐ coordinatore di classe ☐ consiglio di classe ☐ dirigente scolastico ☐ la famiglia della vittima/e ☐ la famiglia del bullo/i	data: _____ data: _____ data: _____ data: _____ data:

	☐ le forze dell'ordine	data:
	☐ altro, specificare:	data:

ALLEGATO 2 - CHECKLIST A CURA DEI REFERENTI SPORTELLI DI ASCOLTO

Sesso	☐ Maschio ☐ Femmina	
Scuola secondaria di primo grado classe frequentata	☐ Prima ☐ Seconda ☐ Terza	
Richiedente	☐ Genitore	☐ Studente (classe____ sez.____)
Numero di accessi allo sportello anno scolastico 2018-19:		
Problematica per la quale viene richiesto il colloquio ed effettuato l'accesso allo Sportello di Ascolto (se possibile specificare le caratteristiche delle problematiche rilevate):		
Difficoltà di apprendimento:		
Difficoltà relazionali con i compagni:		
Bullismo, Cyberbullismo:		
Difficoltà relazionali con gli insegnanti:		
Difficoltà familiari:		
Difficoltà emozionali (ansia prestazionale, stati depressivi, autolesionismo):		
Difficoltà comportamentali (scarso rispetto delle regole, condotte aggressive, problematiche disciplinari):		
Problematiche alimentari:		
Videodipendenza:		
Altro:		
Il funzionamento globale dello studente (scolastico, relazionale, comportamentale ed emozionale) è interferito dalle problematiche per cui si è rivolto allo sportello?		
☐ in modo rilevante	☐ in modo significativo	
Note relative ai temi emersi nel primo incontro:		

L'accesso allo Sportello di ascolto ha comportato la messa in atto di azioni successive (colloqui con il minore, colloqui con i genitori, richieste di collaborazione dell'equipe insegnanti):	
☐ Si	☐ No
Descrivere le eventuali azioni messe in atto	
Il genitore/lo studente come è venuto a sapere dell'esistenza dello sportello?	☐famiglia ☐docente ☐compagno di classe ☐sito della scuola/locandina a scuola ☐amico/a che non fa parte della sua classe ☐altro, specificare:

ALLEGATO 3 - SCHEMA DI PROCEDIMENTO PER CASO EVIDENTE DI CYBERBULLISMO

<table>
<tr><td colspan="2">Caso di evidenza. Il docente ha evidenza che stia accadendo qualcosa tra gli alunni/e della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo</td></tr>
<tr><td rowspan="2">Se hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in ogni momento una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96 Operativo h 24.</td><td>ATTORI ADULTI DA COINVOLGERE

1. Condividi con il referente per il cyberbullismo (e/o il referente indicato nell’e-Policy): valuta con lui/loro le possibili strategie di intervento.
2. Avvisa il Dirigente Scolastico che convoca il CDC.
3. Se non c’è fattispecie di reato.
• Richiedi la consulenza dello/a psicologo/a scolastico/a a supporto della gestione della situazione, in base alla gravità
• Informa i genitori (o chi esercita la responsabilità genitoriale) dei ragazzi/e direttamente coinvolti (qualsiasi ruolo abbiano avuto), se possibile con la presenza dello psicologo/a, su quanto accade e condividete informazioni e strategie.
• Informa i genitori di ragazzi/e infra quattordicenni della possibilità di richiedere la rimozione, l’oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy).
• Attiva il consiglio di classe.
• Valuta come coinvolgere gli operatori scolastici su quanto sta accadendo.</td></tr>
<tr><td>A seconda della situazione e delle valutazioni operate con referente, dirigente e genitori, segnala alla Polizia Postale:
a) contenuto; b) modalità di diffusione
Se è opportuno, richiedi un sostegno ai servizi territoriali o ad altre Autorità competenti (soprattutto se il cyberbullismo non si limita alla scuola).</td></tr>
<tr><td rowspan="2">Promuovi per l’intera comunità scolastica percorsi di prevenzione dei comportamenti a rischio on line.</td><td>CLASSE/I DA COINVOLGERE

1. Capire il livello di diffusione dell’episodio a livello di Istituto e parla della necessità di non diffondere ulteriormente online i materiali.
2. Dialoga (con la classe - 1): Parla del cyberbullismo e delle sue conseguenze (non nominare gli alunni coinvolti). Suggerisci di chiedere aiuto per situazioni di questo tipo. Prevedi un momento laboratoriale in modo da facilitare l’elaborazione della situazione.
3. Dialoga (con la classe - 2): a seconda della situazione trova il modo di supportare la vittima e di responsabilizzare i compagni,
rispetto al loro ruolo, anche di spettatori, nella situazione. A seconda del livello di diffusione anche nelle altre classi.</td></tr>
<tr><td>Tieni traccia di quanto successo e delle azioni intraprese: compila il diario di bordo.</td></tr>
</table>

ALLEGATO 4 - MODULO DI SEGNALAZIONE AL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Con questo modello si può richiedere al Garante per la protezione dei dati personali di disporre **il blocco/divieto della diffusione online di contenuti ritenuti atti di cyberbullismo** ai sensi dell'art. 2, comma 2, della legge 71/2017 e degli artt. 143 e 144 del d.lgs. 196/2003.

Inviare
a: Garante per la protezione dei dati personali **indirizzo e-mail:**
cyberbullismo@gpdp.it

IMPORTANTE La segnalazione può essere presentata direttamente da chi esercita la responsabilità genitoriale su un minore.

CHI EFFETTUA LA SEGNALAZIONE?
(Scegliere una delle due opzioni e compilare TUTTI i campi)

□ Inserire studente in prima persona	Nome e Cognome _____ nato/a a _____ il _____ Residente a _____ Via/Piazz Telefono _____	
□ Ho responsabilità genitoriale su un minore che si ritiene vittima di cyberbullismo	Nome e Cognome _____ nato/a _____ il _____ Residente _____ Via/Piazza _____ Telefono _____	
In cosa consiste l'azione di cyberbullismo di cui ti ritieni vittima? indicare una o più opzioni nella lista a lato	☐pressioni ☐aggressione ☐molestia ☐ricatto	☐ingiuria ☐denigrazione ☐diffamazione ☐altro
Quali sono i contenuti che vorresti far rimuovere o oscurare sul web o su un social network? Perché li consideri atti di cyberbullismo? (inserire una descrizione sintetica - importante spiegare di cosa si tratta)	_____ _____ _____ _____ _____	

_____

Dove sono stati diffusi i contenuti offensivi?	□ sul sito internet *(è necessario indicare l'indirizzo del sito o meglio la URL specifica):* _____ □ su uno o più social network *(specificare su quale/i social network e su quale/i profilo/i o pagina/e in particolare):* _____ □ altro *(specificare):* _____

Se possibile, allegare all'e-mail immagini, video, *screenshot* e/o altri elementi informativi utili relativi all'atto di cyberbullismo e specificare qui sotto di cosa si tratta.

1) _____

2) _____

3) _____

HAI SEGNALATO AL TITOLARE DEL TRATTAMENTO O AL GESTORE DEL SITO WEB O DEL SOCIAL NETWORK CHE TI RITIENI VITTIMA DI CYBERBULLISMO RICHIEDENDO LA RIMOZIONE O L'OSCURAMENTO DEI CONTENUTI MOLESTI?

□ Si, ma il titolare/gestore non ha provveduto entro i tempi previsti dalla Legge 71/20017 sul cyberbulllismo *[allego copia della richiesta inviata e altri documenti utili]*;

□ No, perché non ho saputo/potuto identificare chi fosse il titolare/gestore

HAI PRESENTATO DENUNCIA/QUERELA PER I FATTI CHE HAI DESCRITTO?

□ Si, presso _____

□ No

_____, _____ _____

Luogo, data *Nome e Cognome*

Informativa ai sensi dell'art. 13 del Codice inmateria di protezione dei dati personali

Il Garante per la protezione dei dati personali tratterà i dati personali trasmessi, con modalità elettroniche e su supporti cartacei, per lo svolgimento dei compiti istituzionali nell'ambito del contrasto del fenomeno del cyberbullismo. Il loro conferimento è obbligatorio ed in assenza degli stessi la segnalazione/reclamo potrebbe non poter essere istruita. I dati personali potrebbero formare oggetto di comunicazione ai soggetti coinvolti nel trattamento dei dati personali oggetto di segnalazione/reclamo (con particolare riferimento a gestori di siti internet e social media), all'Autorità giudiziaria o alle Forze di polizia ovvero ad altri soggetti cui debbano essere comunicati per dare adempimento ad obblighi di legge. Ciascun interessato ha diritto di accedere ai dati personali a sé riferiti e di esercitare gli altri diritti previsti dall'art. 7 del Codice.

ALLEGATO 5 -LINEE GUIDA PER I RAGAZZI DI UTILIZZO DI INTERNET

1. **FAI ATTENZIONE** perché rimane sempre traccia di quello che posti o scrivi su internet;
2. **STAI ATTENTO** a chi vuol sapere troppe cose. Non dare a nessuno informazioni personali e della famiglia (nome, cognome, età, indirizzo, numero di telefono, nome e orari della scuola, nome degli amici).
3. **CHIEDI SEMPRE IL PERMESSO** prima di inviare o pubblicare su una chat, un social o su una app, qualsiasi materiale in cui ci siano altre persone (foto, video, commenti, etc);
4. **CHIEDITI** se vorresti esserci tu al suo posto quando fai commenti, metti foto o video di/su altri.
5. **NON RISPONDERE alle offese** ed agli insulti;
6. **CONSERVA E SALVA le comunicazioni offensive**, ti potrebbero essere utili per dimostrare quanto ti è accaduto;
7. Se ricevi materiale offensivo (e-mail, sms, mms, video, foto, messaggi vocali) **NON DIFFONDERLO**: potresti essere accusato di cyberbullismo;
8. Rifletti prima di inviare: ricordati che tutto ciò che invii **su internet** diviene pubblico e **rimane per SEMPRE**;
9. Quando sei connesso alla rete **RISPETTA SEMPRE GLI ALTRI:** ciò che per te è un gioco può rivelarsi offensivo per qualcun altro;
10. SE PARTECIPI A GRUPPI in cui leggi offese, dillo ai tuoi genitori o insegnanti, fai *screenshot*, salva il materiale e poi esci dal gruppo.
11. **Riferisci al tuo insegnante o ai tuoi genitori** se qualcuno ti invia immagini che ti infastidiscono e non rispondere; riferisci anche al tuo insegnante o ai tuoi genitori se ti capita di trovare immagini di questo tipo su Internet;
12. Ricordati che se qualcuno ti offende pesantemente puoi ricorrere alla Dirigente Scolastica, al Referente del bullismo, ai tuoi genitori e anche alla Polizia Postale
13. Ricordati che **è facile mentire su internet.** Alcune persone possono fingersi per quello che non sono. Anche le immagini web possono essere false.
14. **PENSA** prima di mettere qualsiasi cosa su internet. NON pubblicare, inviare o condividere materiale imbarazzante o dannoso e inopportuno.
15. Tutti quelli che osservano senza far nulla diventano **corresponsabili delle azioni** del cyberbullo; mettere un *like* su un social o condividere o commentare foto o video sottopone chi lo fa a una responsabilità maggiore.
16. **Rispettate la privacy altrui.** State attenti soprattutto a non pubblicare informazioni personali relative ad altri (comprese immagini, foto o video) senza il loro consenso.
17. La privacy non vi protegge se commettete atti di cyberbullismo su qualcuno (offese, messaggi volgari, foto private e intime)
18. Utilizza password sicure (lunghe con numeri e lettere) tienile riservate. Se vedi cose strane cambiale.
19. **Non scaricare** (senza parlarne con gli adulti) - loghi, suonerie, app, immagini o file in genere, sia da Internet che come allegati a messaggi di posta elettronica, che

possono creare intromissioni nel computer, ovvero possono comportare costi o addebiti indesiderati.

ALLEGATO 6- LINEE GUIDA PER I GENITORI DI UTILIZZO DI INTERNET

Consigli per difendere i propri figli dai pericoli legati all'uso delle nuove tecnologie Molti bambini utilizzano internet già durante i primi anni della scuola primaria (6-7 anni). È importante sottolineare che è fondamentale l'accompagnamento all'utilizzo di internet da parte di un adulto (genitore, insegnante, educatore) in relazione all'età del bambino. I bambini al di sotto dei 10-11 anni, in genere, non avendo ancora sviluppato le capacità di pensiero critico necessarie, non sono in grado di esplorare il web da soli. scaricano musica, utilizzano motori di ricerca per trovare informazioni, visitano siti, inviano e ricevono sms, la posta elettronica e i giochi online. La supervisione degli adulti è quindi fondamentale anche in questa fase, poiché una maggior conoscenza e consapevolezza legate alla crescita non mettono comunque al riparo dai rischi della Rete.

- Chiedete ai vostri figli di essere informati rispetto alla loro attività in rete: cosa fanno e con chi stanno condividendo;
- Ricordatevi che siete responsabili fino ai 14 anni dell'utilizzo che fanno del loro *smartphone*;
- Utilizzate app di condivisione (tipo *whatsapp*) tra genitori in modo consono allo scopo per cui vengono creati i gruppi, utilizzando modalità comunicative appropriate;
- Stabilite i tempi di utilizzo del computer e del collegamento in rete secondo l'età del minore; condividete con lui le raccomandazioni e le regole di utilizzo dello *smartphone* per un uso consapevole e corretto;
- Creare un rapporto di dialogo con il minore, essere disponibili, farsi raccontare dei suoi contatti e dei suoi interessi in rete (siti visitati, chat, ricerche e scoperte effettuate);
- Di tanto in tanto controllare i contenuti postati su Internet dai vostri figli;
- Non lasciare da soli i ragazzi nell'utilizzo dello *smartphone*, soprattutto se frequentano la primaria
- Fate in modo di non lasciare a loro disposizione lo *smartphone* di notte;
- Utilizzate applicativi che possano aiutarvi nel controllo dello *smartphone*;
- Parlate apertamente dei rischi che si possono correre utilizzando internet e *whatsapp*;
- Controllate la cronologia o gli applicativi scaricati sul loro *smartphone*;
- Dite di non dare mai dati personali in rete;
- Ditegli di non rispondere agli insulti perché cosi diventa anche lui colpevole;
- Ricordategli che tutti i cellulari o pc lasciano una traccia che può essere trovata dalla Polizia;
- Ricordategli che le cose scritte o alcune fotografie, POSSONO FAR PIÙ MALE perché rimangono SEMPRE;
- Fate presente che molti comportamenti illeciti che loro conosco nel reale (insultare, offendere, fotografare di nascosto, accedere illecitamente ad un servizio, etc) lo sono anche nel virtuale;
- Fate presente e insistete che qualcosa messo su internet è incancellabile;
- Salvate sul computer il materiale che può fungere da prova (per esempio screenshot, conversazioni in chat e immagini) e subito dopo, se possibile, cancellare - o far cancellare dal gestore della piattaforma - tutti i contenuti in rete;

- Se sono coinvolti compagni di scuola, i genitori dovrebbero rivolgersi agli insegnanti e, laddove presente, allo psicologo scolastico per valutare se sporgere denuncia presso la polizia.

Link
www.commissariatops.it
www.generazioniconnesse.it

ALLEGATO 7- LINEE GUIDA PER LA SCUOLA

Politica d'Uso Accettabile e Sicura della Scuola esemplare (PUA)

La PUA fa parte delle strategie delle TIC (Tecnologie d'Informazione e Comunicazione) e si basa su linee guida delle politiche nazionali. Il Consiglio d'Istituto ha preso atto del documento e lo ha approvato in data 15/02/2017. Il documento è in allegato al regolamento d'Istituto.

Contenuti

1. I vantaggi di internet a scuola
2. Le strategie della scuola per garantire la sicurezza delle TIC
3. Accertamento dei rischi e valutazione dei contenuti di internet
4. Norme e linee guida
   4.1. Fornitore dei servizi di posta elettronica
   4.2. La gestione del sito della scuola
   4.3. Mailing list con il moderatore, gruppi di discussione e chat room
   4.4. Altre tecnologie di comunicazione
5. Informazioni sulla PUA della scuola
   5.1. Informazioni per gli studenti sulla PUA della scuola
   5.2. Informazioni per il personale scolastico sulla PUA della scuola
   5.3. Informazioni per i genitori/tutori sulla PUA della scuola

1. I vantaggi di internet a scuola

Il curricolo scolastico prevede che gli studenti imparino a trovare materiale, recuperare documenti e scambiare informazioni utilizzando le TIC. Internet offre sia agli studenti che agli insegnanti una vasta scelta di risorse diverse e opportunità di scambi culturali con gli studenti di altri paesi. Inoltre, su internet si possono recuperare risorse per il tempo libero, le attività scolastiche e sociali.

La scuola propone agli studenti e agli insegnanti di utilizzare internet per promuovere l'eccellenza in ambito didattico attraverso la condivisione delle risorse, l'innovazione e la comunicazione. Per gli studenti e per gli insegnanti l'accesso ad internet è un privilegio e un diritto.

Poiché esiste la possibilità che gli studenti trovino materiale inadeguato e illegale su internet, la scuola ha cercato di prendere delle precauzioni limitando l'accesso ad esso.

Gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività on-line, di stabilire obiettivi chiari e insegnare un uso di internet accettabile e responsabile. L'obiettivo principale resta quello di arricchire ed ampliare le attività didattiche, secondo quanto prevede il curricolo scolastico, l'età e la maturità degli studenti.

2. Strategie della scuola per garantire la sicurezza delle TIC

a. Il sistema informatico delle TIC della scuola viene controllato periodicamente dal responsabile, in base alle norme di sicurezza.
b. La connessione wifi che permette l'accesso ad internet è protetto da una password.
c. Il sistema informatico della scuola è provvisto di un software antivirus aggiornato annualmente.
d. Per ciò che concerne l'utilizzo di chiavette ed hard disk esterni personali, la scuola non risponde di eventuali virus che questi strumenti assorbono.
e. Utilità di sistema e file eseguibili non possono essere utilizzati nelle attività degli studenti.

f. I software installati nei dispositivi elettronici della scuola, vengono controllati periodicamente per evitare un mal funzionamento causato da manomissioni accidentali o volontarie.

3. Accertamento dei rischi e valutazione dei contenuti di internet

La scuola si fa carico di tutte le precauzioni necessarie per garantire agli studenti l'accesso a materiale appropriato. La scuola non può farsi carico della responsabilità per il materiale trovato su internet o per eventuali conseguenze causate dall'accesso ad internet.
Gli studenti imparano ad utilizzare i metodi di ricerca su internet, che includono i cataloghi per soggetto e l'uso dei motori di ricerca. Ricevere e inviare informazioni o messaggi e-mail prevede una buona abilità di gestione delle informazioni e di comunicazione. Le abilità di gestione delle informazioni includono:

1. Garanzia di validità, la diffusione e l'origine delle informazioni a cui si accede o che si ricevono;
2. Utilizzazione di fonti alternative di informazione per proposte comparate;
3. Ricerca del nome dell'autore, dell'ultimo aggiornamento del materiale, e dei possibili altri link al sito;
4. Rispetto dei diritti d'autore e dei diritti di proprietà intellettuale. Gli studenti devono essere pienamente coscienti dei rischi a cui si espongono quando sono in rete. Devono essere educati a riconoscere ed evitare gli aspetti negativi di internet come la pornografia, la violenza, il razzismo e lo sfruttamento dei minori. Agli studenti non dovrebbe essere sottoposto materiale di questo tipo e se ne venissero a contatto dovrebbero sempre riferire l'indirizzo internet (URL) all'insegnante del momento o al referente delle TIC.

4. Norme e linee guida

Tutti gli utenti connessi ad internet devono aderire alla legislazione vigente applicata anche alla comunicazione su internet. I computer della scuola ai quali è data possibilità agli studenti di accesso, hanno filtri adeguati per evitare chat non moderate, gruppi di discussione o siti web con contenuto pornografico.
Per tutti c'è l'obbligo di **NON** accedere a siti diseducativi; effettuare ricerche di pagine o siti web in modo dinamico, con l'uso di parole chiave inappropriate; alterare le impostazioni del browser che respingono le pagine con contenuto pornografico o simili.

4.1. Fornitore di servizi internet

1. Gli studenti dovrebbero riferire agli insegnanti se ricevono e-mail offensive.
2. Tutti gli studenti hanno un account d'Istituto sul quale possono lavorare con le applicazioni di Google.
2. È vietato utilizzare catene di messaggi telematiche senza il permesso del mittente.
3. Gli studenti possono accedere ad internet, vedere file o mail, fare ricerche, o altro, solo se autorizzati dal docente.
4. Gli studenti non devono pubblicizzare dati sensibili, indirizzi, numeri di telefono di altre persone di loro conoscenza senza il loro permesso.
5. L'invio e la ricezione di allegati è soggetto al permesso dell'insegnante.

4.2. Gestione del sito web della scuola

La Dirigente della scuola gestisce le pagine del sito ed è sua responsabilità garantire che il contenuto sul sito sia accurato e appropriato. Il sito assolverà alle linee guida sulle pubblicazioni della scuola.

La scuola detiene i diritti d'autore dei documenti che si trovano sul sito, oppure se è stato chiesto ed ottenuto il permesso, all'autore proprietario.
Le informazioni pubblicate sul sito della scuola relative alle persone da contattare devono includere solo l'indirizzo della scuola, l'indirizzo di posta elettronica e il telefono della scuola, ma non informazioni relative agli indirizzi del personale della scuola o altre informazioni del genere.
Le fotografie degli studenti non verranno pubblicate senza il consenso scritto dei loro genitori o tutori e il nome degli studenti non verrà allegato alle fotografie.

4.3. Mailing List moderate, gruppi di discussione e Chat Room

La scuola può utilizzare una lista di indirizzi di utenti selezionati per distribuire del materiale. L'insegnante è il moderatore degli altri mezzi di collaborazione, dei gruppi di discussione e delle *Chat Room* se sono utilizzati a scuola.

1. Agli studenti non è consentito l'accesso alle *Chat Room* pubbliche o non moderate.

2. Sono permesse solo *Chat* a scopi didattici e comunque sempre con la supervisione dell'insegnante per garantire la sicurezza.
3. Solo i gruppi di discussione che hanno obiettivi e contenuti didattici sono disponibili agli studenti.

4.4. Altre forme tecnologiche di comunicazione

Agli studenti non è permesso tenere acceso gli *smartphone* durante le lezioni o durante l'orario scolastico, senza il permesso del docente. Si ribadisce il concetto che in ogni caso l'uso di queste apparecchiature è prettamente didattico.

5. Informare sulla Politica d'Uso Accettabile (PUA) della scuola

5.1.Informare gli studenti sulla PUA della scuola

Le regole di base relative all'accesso ad internet verranno esposte vicino al laboratorio di informatica; inoltre tutti gli studenti saranno informati che l'utilizzo di internet è monitorato e gli verranno date delle istruzioni per un uso responsabile e sicuro.

5.2. Informare il personale scolastico della PUA

Il documento verrà pubblicato sul sito web della scuola oltre che in allegato al Regolamento d'Istituto; il personale scolastico sarà consapevole che l'uso di internet verrà monitorato. Viene richiesto a tutto il personale scolastico di contribuire all'applicazione delle istruzioni sull'uso sicuro e responsabile di internet come descritto dal documento.
In caso di dubbi legati alla legittimità di una certa istanza utilizzata in internet, l'insegnante dovrà contattare il Dirigente o il referente delle TIC per evitare malintesi. Gli insegnanti hanno il dovere di conoscere le regole che governano i diritti d'autore applicate dalla scuola (es. Sito web dell'Istituto).

5.3. Informare i genitori/tutori sulla PUA della scuola

I genitori potranno prendere visione del documento PUA nel sito web della scuola.

Documento approvato dal Consiglio di Istituto ed allegato al Regolamento d'Istituto con Delibera n. 91 del 15/02/2017.

ALLEGATO 8 – ATTESTATO DI QUALIFICA "SCUOLA VIRTUOSA"

Direzione Generale per lo Studente l'Integrazione e la Partecipazione

Generazioni Connesse SAFER INTERNET CENTRE

Co-financed by the European Union Connecting Europe Facility

GENERAZIONI CONNESSE (SIC ITALY III)

Preso atto che l'**Istituto Comprensivo "G.Micali" di Livorno** ha svolto il percorso con l'aiuto del Safer Internet Centre Italia, elaborando una propria **policy di E-SAFETY**, indicante 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,

SI ATTESTA

l'esito positivo della partecipazione al Progetto e la qualifica di "***scuola virtuosa***" sui temi relativi all'uso sicuro e positivo delle tecnologie digitali, utile ai fini della descrizione del proprio curriculo. Il nominativo dell'Istituto verrà pubblicato sul sito del Progetto: www.generazioniconnesse.it

Roma, 30 Novembre 2018

IL DIRIGENTE
Giuseppe PIERRO

