



**ISTITUTO COMPRENSIVO DI SISSA TRECASALI**

Piazzale Gianni Rodari n. 1 Loc. Trecasali - 43018 Sissa Trecasali (PR)

Sito WEB: [www.icsissatrecasali.it](http://www.icsissatrecasali.it) Tel. 0521/878301

PEO: [pric805003@istruzione.it](mailto:pric805003@istruzione.it) - PEC: [pric805003@pec.istruzione.it](mailto:pric805003@pec.istruzione.it)



# E-Safety

## POLICY

**PER UN USO CONSAPEVOLE DEGLI STRUMENTI  
DIGITALI**

## INDICE

### **Capitolo 1 - Presentazione dell'ePolicy**

1. Introduzione
2. Scopo dell' E- Policy
3. Ruoli e responsabilità nell'implementazione dell'E-Policy
4. Condivisione, Monitoraggio e Aggiornamento dell'E-Policy
5. Integrazione dell' E-Policy con regolamenti e normativa generale esistenti
6. Gestione delle infrazioni della policy.
7. I Piani di Azione dell' E- Policy
8. Le risorse di Generazioni Connesse

### **Capitolo 2 - Sensibilizzazione e prevenzione**

1. Curricolo Digitale
2. Formazione dei docenti sull'utilizzo consapevole e sicuro di internet e delle tecnologie digitali
3. Il Kit Didattico

### **Capitolo 3 - Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola**

1. Protezione dei dati personali e GDPR
2. Strumenti di comunicazione online (PUA)
3. Strumentazione personale (BYOD)

### **Capitolo 4 - Rischi ONLINE: Conoscere, Prevenire E Rilevare**

1. Strategie di intervento
2. La rilevazione
3. Segnalazione e Gestione dei casi
4. Allegati con le procedure

## **1.1 - INTRODUZIONE**

La Policy E-Safety è un documento programmatico della scuola, il cui fine è diffondere strumenti e misure per promuovere l'utilizzo positivo delle TIC nella didattica e negli ambienti scolastici e prevenire e gestire le situazioni problematiche che possono sorgere per l'uso delle tecnologie digitali.

In una società, sempre più digitale, reticolare, ipercomplessa, l'Istituto Comprensivo di Sissa Trecasali si "ri-innova", estendendo il concetto stesso di scuola da luogo fisico a spazio di apprendimento virtuale. Una riconfigurazione funzionale degli ambienti per l'apprendimento che seguono la direzione di una visione sostenibile, collaborativa e aperta di scuola.

La policy è, attraverso le sue azioni, una richiesta di sforzo collettivo che mira a valorizzare e potenziare la partecipazione responsabile di tutte le figure e le istituzioni interessate, definendo ruoli e responsabilità condivise.

Il documento segue le indicazioni delle Linee di Orientamento per la prevenzione e il contrasto del bullismo e cyberbullismo aggiornate con decreto n.18 del 13/01/2021 e relativa nota prot. 482 del 18.02.2021 elaborate dal Ministero dell'Istruzione e del Merito nonché la L.70 del 2024 che ha novellato la legge 29 maggio 2017, n. 71.

## **1.2 - SCOPO DELL'E-POLICY**

L'E-policy ha come finalità principale quello di promuovere le competenze digitali per un uso delle tecnologie digitali positivo, critico e consapevole, da parte degli studenti e delle studentesse guidati dagli adulti coinvolti nel processo didattico-educativo.

L'E-policy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.

Le TIC (Tecnologie dell'informazione e della comunicazione) rappresentano nella società odierna strumenti fondamentali nel processo educativo e per l'apprendimento degli studenti e delle studentesse. La competenza digitale è una competenza chiave del cittadino europeo come indicato dal Consiglio Europeo (Raccomandazione del 2018) che permette ad ogni cittadino di esercitare i propri diritti all'interno degli ambienti digitali (ONU - Commento Generale 25: I diritti dei minori negli ambienti digitali).

L'IC di Sissa Trecasali mediante l'E-Policy vuole rappresentare la visione educativa e la proposta formativa adottate in riferimento alle tecnologie digitali.

Nello specifico:

- l'approccio didattico educativo alle tematiche connesse alle "competenze digitali", alla privacy, alla sicurezza online e all'uso delle tecnologie digitali;
- Il piano di azioni triennale per promuovere nell'intera comunità scolastica l'uso sicuro responsabile e positivo della rete;

- le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
- le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
- le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

### 1.3 - RUOLI E RESPONSABILITÀ NELL'IMPLEMENTAZIONE DELL'E-POLICY

**L'Istituto Comprensivo di Sissa Trecasali dichiara fermamente l'inaccettabilità di qualsiasi atto di violenza, prepotenza, offesa e di 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 online 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). L'Istituto si impegna, attraverso i propri regolamenti, il patto di corresponsabilità e le strategie educative, a costruire una comunità attenta a salvaguardare l'**interesse superiore del minore**. Affinché l'E-policy sia davvero uno strumento operativo efficace per la scuola e tutta la comunità educante è necessario che ognuno, secondo il proprio ruolo, si attenga a quanto di seguito indicato.

#### Il Dirigente Scolastico

Il Dirigente Scolastico, in qualità di rappresentante legale dell'istituto e garante delle opportunità formative:

- attiva iniziative e interventi tesi a favorire l'educazione all'uso consapevole della rete internet tramite appositi progetti, aventi carattere di continuità tra i diversi gradi di istruzione ed elaborati singolarmente o in rete, in collaborazione con enti locali, servizi territoriali, organi di polizia, associazioni ed enti;
- incentiva attività che si pongono l'obiettivo di prevenire e contrastare i fenomeni del bullismo e del cyberbullismo in tutte le loro manifestazioni, con azioni a carattere preventivo e con una strategia di attenzione, tutela nei confronti dei minori coinvolti, sia nella posizione di vittime sia in quella di responsabili di illeciti, privilegiando azioni di carattere formativo ed educativo e assicurando l'attuazione degli interventi, senza distinzione di età, nell'ambito delle istituzioni scolastiche.(art.1 della L.70/2024);
- promuove la collaborazione tra le organizzazioni degli enti locali, sportive e del Terzo settore che svolgono attività educative, anche non formali, e nei riguardi dei soggetti esercenti la responsabilità genitoriale, cui incombe l'obbligo di orientare i figli al corretto utilizzo delle tecnologie e di presidiarne l'uso;

- instaura intese con i servizi territoriali (servizi della salute, servizi sociali, forze dell'ordine, servizi minorili dell'amministrazione della Giustizia) per un supporto specializzato e continuativo ai minori coinvolti ove necessario;
- apporta modifiche e integrazioni al Regolamento di Istituto e al Patto di Educativo Corresponsabilità, con specifici riferimenti a misure preventive verso i comportamenti di cyberbullismo e relative sanzioni disciplinari proporzionate alla gravità degli atti compiuti;
- individua fra i docenti un referente e nomina un team antibullismo con il compito di coordinare e attuare iniziative di prevenzione e di contrasto al bullismo e al cyberbullismo;
- adotta le “Linee di Orientamento per la prevenzione e il contrasto del Bullismo e Cyberbullismo - aggiornamento 2021 - per le istituzioni scolastiche di ogni grado. attivando iniziative di formazione per il personale scolastico e promuovendo un ruolo attivo degli studenti, nonché di ex studenti che abbiano già operato all'interno dell'istituto scolastico in attività di peer education, nella prevenzione e nel contrasto del cyberbullismo nelle scuole;
- si impegna inoltre ad informare tempestivamente, i genitori dei minori coinvolti (o chi ne esercita la responsabilità genitoriale o i tutori) qualora venga a conoscenza di atti di bullismo e cyberbullismo che non si configurino come reato;
- assicura l'informazione alle famiglie delle attività e iniziative intraprese anche mediante il sito web della scuola;
- promuove la cultura della sicurezza online anche attraverso uno strumento che possa lavorare sulla prevenzione, rilevazione, gestione dei casi (E-Policy);
- garantisce l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza on line;
- garantisce la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri della comunità scolastica;
- garantisce ai docenti una formazione di base sulle Tecnologie dell'Informazione e della Comunicazione (ICT) tale da consentire loro il possesso delle competenze necessarie all'utilizzo di tali risorse.

## **L'ANIMATORE DIGITALE E IL TEAM PER L'INNOVAZIONE DIGITALE**

L'animatore digitale e il Team per l'Innovazione digitale sono co-responsabili, con il referente del Referente Prevenzione Bullismo-Cyberbullismo- Legalità, dell'attuazione dei piani di azione in particolare in riferimento alla formazione dei docenti. Sono inoltre responsabili del controllo all'accesso da parte degli studenti delle TIC.

Di seguito le azioni da mettere in campo:

- stimolare la formazione interna alla scuola negli ambiti del PNSD, attraverso l'organizzazione di laboratori formativi, favorendo l'animazione e la partecipazione di tutta la comunità scolastica alle attività formative;
- favorire la partecipazione e stimolare il protagonismo degli studenti nell'organizzazione di workshop e altre attività, anche strutturate, sui temi del PNSD, con momenti formativi aperti alle famiglie e ad altri attori del territorio, per la realizzazione di una cultura digitale condivisa;
- individuare soluzioni metodologiche e tecnologiche sostenibili da diffondere all'interno degli ambienti della scuola (es. uso di particolari strumenti per la didattica di cui la scuola si è dotata; adozione di metodologie comuni; informazione su innovazioni esistenti in altre scuole; laboratorio di coding per tutti gli studenti), coerenti con l'analisi dei fabbisogni della scuola stessa, anche in sinergia con attività di assistenza tecnica condotta da altre figure.

## **IL REFERENTE PREVENZIONE BULLISMO-CYBERBULLISMO- LEGALITA'**

La legge n. 71/2017 prevede la figura di un coordinatore delle iniziative di prevenzione e contrasto del cyberbullismo messe in atto dalla scuola. Tale figura è il referente di Istituto: *"Ogni istituto scolastico, nell'ambito della propria autonomia, individua fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo ..."* ( art. 4 comma 3). Compito del referente è di coordinare le iniziative di prevenzione e contrasto del cyberbullismo anche in collaborazione con Forze di Polizia, associazioni e centri di aggregazione giovanile presenti sul territorio. Cura inoltre i rapporti di rete fra scuole per eventuali convegni/seminari/corsi e per la giornata mondiale sulla Sicurezza in Internet la "Safer Internet Day" per una disseminazione di buone pratiche preventive che coinvolgano la comunità scolastica. Svolge inoltre supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'Istituto), atti e documenti (PTOF, PdM, Rav). Il referente cyberbullismo è co-responsabile, con il team antibullismo, dell'attuazione dei piani di azione e coordina le iniziative di prevenzione e contrasto del bullismo e cyberbullismo.

## **IL TEAM ANTIBULLISMO E PER L'EMERGENZA**

In coerenza con le Linee di Orientamento per la prevenzione e il contrasto del Bullismo e Cyberbullismo del Ministero dell'Istruzione (D.M. n. 18 del 13/1/2021, agg. 2021 – nota prot. 482 del 18-02-2021), il Team ha le funzioni di coadiuvare il Dirigente Scolastico nella definizione degli interventi di prevenzione e nella gestione dei casi di bullismo e cyberbullismo che si possono presentare. Ha altresì il compito di:

- Intervenire nelle situazioni acute di bullismo e cyberbullismo;
- Promuovere la redazione e l'applicazione della ePolicy e monitorare le segnalazioni.

## I/LE DOCENTI

I docenti, in coerenza con la normativa vigente, si impegnano a intraprendere percorsi formativi di **Media Education** al fine di:

- **educare ai media (teaching about the media):** i media sono l'oggetto dell'intervento educativo, si mira a promuovere una riflessione critica approfondendo le tematiche inerenti il sistema dei media, la decodifica dei messaggi e la conoscenza dei linguaggi mediali. Gli alunni verranno guidati ad un corretto accesso alle TIC, condividendo la **netiquette** e dando regole e codici di comportamento condivisi e trasparenti.
- **educare con i media (teaching with the media):** in questo caso i media sono considerati come strumenti attraverso cui realizzare l'intervento formativo. Verranno pertanto programmati percorsi di innovazione e digitalizzazione per favorire la creatività e il protagonismo degli studenti nel quadro della valorizzazione delle competenze chiave.

Inoltre sarà compito degli insegnanti:

- mostrarsi fermi nel condannare ogni atto di intolleranza e sopraffazione;
- osservare regolarmente i comportamenti a rischio sia dei potenziali bulli sia delle potenziali vittime con particolare supervisione durante l'intervallo e l'orario di mensa;
- evitare di porsi come unico depositario dell'intervento sul bullo o sui bulli. Nel caso si verificasse un episodio di bullismo e/o cyberbullismo attivare il Referente d'Istituto e dare inoltre immediata comunicazione al Dirigente Scolastico. È necessario poi coinvolgere i genitori convocandoli per un colloquio e il Consiglio di Classe, al fine di definire soluzioni specifiche condivise;
- mantenere tutte le comunicazioni digitali con alunne/alunni e genitori/tutori a livello professionale e realizzarle esclusivamente con sistemi ufficiali scolastici;
- assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- sviluppare le competenze digitali degli alunni e fare così in modo che conoscano e seguano le norme di sicurezza nell'utilizzo del web e utilizzino correttamente le tecnologie digitali sia a scuola sia nelle attività didattiche extracurricolari;
- controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche ecc. nelle lezioni e nelle altre attività scolastiche che ne prevedono la necessità a scopi didattici;
- tenere un diario di bordo per monitorare la casistica e la situazione problematica degli episodi di cui siete a conoscenza e dei loro sviluppi;
- pianificare sempre la navigazione di studentesse e studenti, nelle lezioni in cui è previsto l'uso di Internet, verso siti controllati come idonei per evitare di incontrare materiali inadatti;

- sviluppare le competenze prosociali integrando la classe “COGNITVA” con la classe “AFFETTIVO-RELAZIONALE” investendo quindi sulle strategie di coping, sulla resilienza, sulla gestione dei conflitti, sull'empatia, sulla responsabilità, sullo sviluppo del senso morale-civico, sull'autodisciplina;
- promuovere l'uso delle TIC per l'INCLUSIONE: **“Il potenziale di questi strumenti può contribuire a ridurre l'esclusione sociale e aumentare la partecipazione, aspetto riconosciuto a livello internazionale, ma sono anche note le barriere sociali, economiche e politiche che il mancato accesso alle nuove tecnologie può generare” (Vertice Mondiale sulla Società dell'Informazione – WSIS, 2010).**
- informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet con particolare riferimento alla dimensione etica (tutela della privacy, rispetto dei diritti dei materiali reperiti in Internet e dell'immagine degli altri, lotta al cyberbullismo) e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento.

## IL DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI:

Il Direttore dei Servizi Generali e Amministrativi dovrà:

- assicurare, nei limiti delle risorse finanziarie disponibili, gli interventi di manutenzione richiesti da cattivo funzionamento e/o danneggiamento della dotazione tecnologica dell'Istituto, controllando al contempo che le norme di sicurezza vengano rispettate;
- facilitare la trasmissione di comunicazioni relative alle tecnologie digitali tra le varie componenti della scuola (Dirigente scolastico, Animatore digitale, docenti e famiglie degli alunni);
- curare la registrazione dei disservizi e delle problematiche relative alla rete e all'uso del digitale segnalate dai docenti, provvedendo all'intervento del personale tecnico di assistenza.

## IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)

Il Personale ATA è tenuto a partecipare attivamente alle iniziative formative messe in atto dalla scuola circa la conoscenza dei rischi, le misure di prevenzione e protezione che si possono mettere in campo riguardo la sicurezza informatica. È fatto d'obbligo segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico o al Referente di Istituto per le opportune azioni ed eventuali sanzioni e mantenere tutte le comunicazioni digitali con alunne/alunni e genitori/tutori a livello professionale e realizzarle esclusivamente con sistemi ufficiali scolastici.

## IL RESPONSABILE DELLA PROTEZIONE DEI DATI

Il Responsabile della protezione dei dati (RPD o DPO) conosce l'ePolicy di Istituto, fornisce la propria consulenza in merito agli obblighi derivanti dal GDPR e sorveglia sull'esatta osservanza della normativa in materia di tutela dei dati personali ed è co-responsabile delle azioni di informazione e formazione nell'Istituto sulla protezione dei dati personali.

## GLI STUDENTI E LE STUDENTESSE

Gli studenti e le studentesse devono, in relazione al proprio grado di maturità e consapevolezza raggiunta, sono responsabili per l'utilizzo corretto dei sistemi informatici e della tecnologia digitale in accordo con i termini previsti da questa policy. In particolare sono tenuti a:

- acquisire le buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali in tutti i momenti della vita, per la propria e altrui incolumità;
- partecipare attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e farsi promotori di quanto appreso anche attraverso possibili percorsi di peer education;
- migliorare le proprie conoscenze, abilità e competenze nell'uso delle TIC per divenire cittadini digitali responsabili;
- essere a conoscenza che non si possono usare cellulari, smartphone, riproduttori di musica, durante le attività didattiche se non per finalità didattiche e sempre previo consenso del docente;
- essere consapevoli che non è loro consentito, all'interno della scuola, acquisire e diffondere mediante telefonini cellulari o altri dispositivi elettronici, immagini, filmati o registrazioni vocali (**tutela dei dati personali**);
- comprendere l'importanza di essere responsabili nel segnalare ogni forma di abuso, uso improprio, accesso a materiali inappropriati di cui si è testimoni;
- maturare un pensiero critico e riflessivo riguardo i social, internet, le webapp che implica dovere e responsabilità verso sé stessi e verso gli altri, nella partecipazione (**netiquette**);
- essere a conoscenza che, con l'entrata in vigore del Nuovo Regolamento UE sulla Privacy (Gdpr) dal **25 maggio 2018** le principali piattaforme hanno cambiato le condizioni d'uso sul consenso al trattamento dei dati personali. Inoltre, chi ha meno di 16 anni e vuole usare questi servizi, dovrà avere un genitore o tutore che acconsenta a suo nome in termini di utilizzo. Si rammenta che quasi tutte le app social (Facebook, Twitter, Whatsapp, Instagram...) sono vietati a chi ha meno di 13 anni in base al **Children's Online Privacy Protection Act del 1998 (USA)**.
- saper "staccare la spina". In base ai dati dell'Associazione DI.TE.( Associazione Nazionale Dipendenze Tecnologiche) **il 51% dei giovani tra i 15 e i 20 anni** controlla in media lo **smartphone 75 volte**, **il 7% arriva fino a 110 volte al giorno**.

Dal sondaggio emerge che il **79%** dei ragazzi ha ammesso di non riuscire a prendersi una pausa di almeno tre ore dallo smartphone e altri device. Per i **giovani 3.0** aumenta pertanto il rischio di incorrere in casi di "dipendenza da internet" (la nomofobia, il vamping, l'Hikikomori....)

## **I GENITORI/ADULTI DI RIFERIMENTO**

I Genitori, in continuità con l'Istituto scolastico, sono attori partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile degli strumenti personali (pc, smartphone, etc). Come parte della comunità educante devono possedere piena consapevolezza circa le opportunità e i rischi correlati all'uso delle nuove tecnologie al fine di :

- vigilare sull'uso delle tecnologie da parte dei ragazzi, con particolare attenzione ai tempi, alle modalità, ai comportamenti conseguenti (ad esempio stati depressivi, ansiosi o di paura successivi all'uso di internet);
- insegnare al figlio a chiedere aiuto in caso di bisogno, a riporre fiducia nelle figure di riferimento;
- educare ad un uso critico e responsabile delle tecnologie comunicative: "essere social" non sempre vuol dire "saper socializzare".

Alle famiglie quindi si richiede il compito di:

- partecipare attivamente alle azioni di formazione/informazione, istituite dalle scuole, sui comportamenti sintomatici del bullismo e del cyberbullismo;
- instaurare un'alleanza educativa con docenti e dirigente scolastico basata sulla collaborazione e il rispetto dei ruoli per disseminare le buone pratiche di E-safety Policy e seguire le linee guida sull'uso appropriato di immagini digitali e video registrati in occasione di eventi scolastici, anche al di fuori delle aule;
- conoscere le sanzioni previste da Regolamento d'Istituto nei casi di bullismo, cyberbullismo e navigazione on-line a rischio.

Si promuove il coinvolgimento dei rappresentanti di genitori/adulti di riferimento all'interno del percorso di definizione e implementazione dell' E-Safety Policy.

## **GLI ENTI ESTERNI PUBBLICI E PRIVATI E LE ASSOCIAZIONI - *informativa per i soggetti esterni che erogano attività nell'Istituto***

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio di interesse superiore del minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa.

**Sono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse oltre che quelli legati a tollerare o partecipare a comportamenti di minori che sono illegali, o abusivi o che mettano a rischio la loro sicurezza.**

Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

#### **1.4 - CONDIVISIONE, MONITORAGGIO E AGGIORNAMENTO DELL'E-POLICY**

Questo documento è fatto oggetto di condivisione e diffusione attraverso l'approvazione da parte del Collegio dei Docenti e del Consiglio di Istituto e tramite pubblicazione sul sito web dell'Istituto. La sua applicazione viene monitorata dal Team per l'Innovazione Digitale e dal Referente del Bullismo che ne cura anche eventuali aggiornamenti. L'aggiornamento del documento viene sottoposto all'approvazione del Collegio dei Docenti.

È fondamentale che ciascun attore scolastico (dai docenti agli/lle studenti/esse) si faccia a sua volta promotore del documento.

**Per una maggiore diffusione e condivisione verrà redatta una versione video child friendly del documento per la comunicazione e sensibilizzazione ai\alle bambini\le e ai\alle ragazzi\le.**

#### **1.5 INTEGRAZIONE EPOLICY NEI DOCUMENTI SCOLASTICI**

Il presente documento si integra pienamente con obiettivi e contenuti dei seguenti documenti, che specificano il contesto di attuazione delle politiche dell'Istituto Comprensivo per un uso efficace e consapevole del digitale nella didattica:

- PTOF
- Regolamento d'Istituto
- Regolamento per l'utilizzo dei laboratori.

La presenza dell'ePolicy nell'Istituto scolastico è garanzia, per il territorio, della presenza di un presidio informato, sensibile e attento sulla rete e le tecnologie in relazione con i più giovani.

**Questo Regolamento è da intendersi come parte integrante del Regolamento di Istituto.**

## **1.6 - GESTIONE DELLE INFRAZIONI DELLA POLICY.**

Le infrazioni alla policy possono essere rilevate dal personale scolastico nell'esercizio delle proprie funzioni oppure possono essere segnalate da alunni e genitori al personale scolastico.

La scuola gestirà le infrazioni all'E-policy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni.

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

Si ricorre all'Autorità Giudiziaria solo ed esclusivamente per fatti di tale gravità da non poter essere risolti con strumenti di natura educativa. Ricordiamo che i pubblici ufficiali e gli incaricati di un pubblico servizio hanno l'obbligo di denunciare all'Autorità Giudiziaria la notizia di ogni reato procedibile d'ufficio di cui siano venuti a conoscenza nell'esercizio o a causa delle loro funzioni o del loro servizio (art. 331 cod. procedimento penale).

La denuncia e il referto rappresentano un preciso obbligo di legge e la loro omissione costituisce reato (artt. 361, 362, 365 cod. pen.). Nel caso in cui le infrazioni della policy violino invece le norme previste dal Regolamento di Istituto si procede secondo le indicazioni dello stesso. In particolare:

### **A. Infrazioni degli alunni**

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

- richiamo verbale;
- sanzioni estemporanee commisurate alla gravità della violazione commessa (ad esempio assegnazione di attività aggiuntive da svolgere a casa su tematiche inerenti l'Educazione Civica);
- nota informativa/disciplinare sul diario e sul RE ai genitori e/o convocazione dei genitori per un colloquio con l'insegnante;
- convocazione dei genitori per un colloquio con il Dirigente scolastico.

Le sanzioni invece comportanti l'allontanamento dalla comunità scolastica sono riservate alla competenza del Consiglio di Classe e del Consiglio d'Istituto. In particolare:

- a) i provvedimenti che comportano l'allontanamento dalla comunità scolastica per un periodo inferiore a 15 giorni sono sempre adottati dal CONSIGLIO DI CLASSE;

b) le sanzioni che comportano un allontanamento superiore a 15 giorni, ivi compresi l'allontanamento fino al termine delle lezioni o con esclusione dallo scrutinio finale o la non ammissione all'esame di Stato conclusivo del corso di studi, sono sempre a carico del CONSIGLIO DI ISTITUTO.

Pertanto gli Organi Competenti a comminare le sanzioni sono:

- Docente
- Dirigente Scolastico
- Consiglio di Classe
- Consiglio di Istituto

In linea con lo Statuto delle studentesse e degli studenti, approvato con D.P.R. n. 249 del 24/05/1998 e successive modifiche ed integrazioni i provvedimenti sono sempre temporanei, proporzionati all'infrazione disciplinare e ispirati al principio fondamentale della finalità educativa e "costruttiva" e non solo punitiva della sanzione. I procedimenti tenderanno sempre al rafforzamento del senso di responsabilità e al ripristino di rapporti corretti all'interno della comunità scolastica.

## **B. Infrazioni del personale scolastico**

Le infrazioni alla policy da parte del personale scolastico possono riguardare sia la mancata osservanza delle regole qui descritte sulla gestione della strumentazione, sia la mancata sorveglianza e pronto intervento nel caso di infrazione da parte degli alunni.

## **C. Infrazioni dei genitori: "Culpa in educando"**

Genitori e familiari svolgono un ruolo fondamentale in un'ottica di interiorizzazione delle norme di comportamento e la loro progressiva strutturazione in un sistema di valori personali e sociali. Essi devono svolgere una costante opera educativa, onde realizzare una personalità equilibrata in cui vi sia la capacità di dominare gli istinti, il rispetto degli altri e tutto ciò in cui si estrinseca la maturità personale. (Cass. Civ.- Sent. 22/04/2009; Cass. Civ.- sent.28/08/2009). Principio sancito già nell'art. 30 della Costituzione: *"E' dovere e diritto dei genitori mantenere, istruire ed educare i figli."* I genitori sono pertanto responsabili del danno cagionato dal fatto illecito dei figli minori e rispondono per i loro comportamenti illeciti sia per omessa o carente sorveglianza, sia per oggettive carenze nell'attività educativa rese evidenti dal mancato rispetto delle regole della civile convivenza. **Quindi quali sono le responsabilità dei genitori in caso di bullismo-cyberbullismo? Colpe di natura solidale e non alternative.** Anche se il minore viene affidato alla custodia di terzi (nel caso specifico, gli insegnanti), sollevandoli di fatto dalla culpa in vigilando, non li solleva però dalla culpa in educando. I genitori sono, infatti, tenuti a dimostrare, per liberarsi da responsabilità per il fatto compiuto da minore in un momento in cui lo stesso si trovava soggetto alla vigilanza di terzi, di avere impartito al minore stesso un'educazione adeguata a prevenire comportamenti illeciti. A sancirlo è la Corte di Cassazione (Sez. Civ. Sez. III n. 1251/2000).

Affinché i genitori del minore possano escludere la loro responsabilità è necessario che essi dimostrino l'efficacia del loro impegno educativo. In assenza di tale prova, che non può ridursi all'espressione di un giudizio, rimane ferma la presunzione di responsabilità dei genitori per il fatto illecito del figlio minorenni sancita dall'articolo 2048 del codice civile.

### **1.7 - I PIANI DI AZIONE DELL'E-POLICY**

I piani di azione rappresentano il programma triennale di obiettivi che la scuola intende realizzare per promuovere la conoscenza delle regole e dei protocolli di intervento che sono stati adottati con il documento di E-Policy nella comunità scolastica.

Nei Piani di Azione sono riportati gli impegni e le responsabilità che la scuola si assume per promuovere sui temi dell'educazione civica digitale e dell'utilizzo sicuro e consapevole delle tecnologie e della rete:

- la rilevazione dei bisogni
- le iniziative informative e formative,
- la formazione di docenti, studenti e studentesse e famiglie,
- il monitoraggio e la valutazione delle azioni (laddove possibile, anche all'interno del RAV e nel PdM);

#### **AZIONI (da sviluppare nell'arco del triennio)**

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Diffondere l'ePolicy negli ambienti scolastici, a studenti e studentesse, docenti e famiglie attraverso le versioni friendly dell'ePolicy.
- Effettuare una rilevazione del fabbisogno formativo dei docenti sui temi dell'educazione civica digitale.
- Effettuare una rilevazione di interessi, bisogni e comportamenti delle famiglie sull'uso positivo del digitale.
- Avviare l'introduzione del kit didattico come metodo e risorsa di lavoro.
- Integrare l'ePolicy (norme, regolamenti e procedure) nei documenti dell'Istituto.
- Definizione, a partire da quanto definito nell'ePolicy, delle procedure di segnalazione anche con linguaggio child/youth friendly perché possano essere accessibili a studenti e studentesse.
- Pianificare corsi di formazione e aggiornamento per il personale scolastico, affinché tutti siano preparati a riconoscere e gestire i segnali di disagio legati all'uso delle tecnologie digitali.

- Collaborazione con istituzioni e servizi esterni: Polizia Postale, i Servizi Sociali e altre istituzioni per garantire un intervento tempestivo nei casi più gravi e favorire uno scambio di informazioni utile alla prevenzione.
- Servizi di counseling: Collaborare con professionisti (psicologi, assistenti sociali) per offrire un supporto psicologico strutturato a studenti e famiglie, garantendo un percorso di recupero e prevenzione del disagio.
- Integrare le attività scolastiche in una rete territoriale che promuova interventi congiunti e continui aggiornamenti sul fenomeno.
- Organizzare workshop e seminari rivolti a studenti, docenti e famiglie per approfondire il tema della sicurezza online, del cyberbullismo e dell'uso responsabile della tecnologia.
- Utilizzare campagne informative e giornate di sensibilizzazione per promuovere una cultura digitale consapevole, coinvolgendo anche enti esterni e istituzioni locali.
- Scambio di best practice: Incentivare la condivisione di esperienze e strategie efficaci tra istituti, per migliorare continuamente le procedure di intervento

## 1.8 - Le risorse di Generazioni Connesse

Le Risorse di Generazioni Connesse:

- **Kit Didattico** ( <https://www.generazioniconnesse.it/site/it/il-kit-didattico/> )
- Area formazione (per docenti, famiglie, studenti/sse con ePolicy)
- Canale **Youtube** (webinar, video-stimolo, serie per target differenti)
- Canale **TikTok**
- Canale **Instagram**
- Canale **Facebook**

## Cap 2 - SENSIBILIZZAZIONE E PREVENZIONE

Il nostro Istituto ha attivato una campagna di comunicazione e sensibilizzazione per gli studenti, bambini, educatori, genitori e tutti gli stakeholder interessati alle tematiche della sicurezza online. Anche nei prossimi anni si organizzeranno incontri, dibattiti, momenti di condivisione che offriranno occasione di confronto e discussione sui rischi di "perdersi nella rete" senza una bussola efficace.

Sarà predisposta un'area dedicata alla sicurezza in rete nella quale saranno inseriti guide per genitori, materiali informativi e link di video collegata alla homepage del sito scolastico (<https://www.icsissatreacasali.it/> ). La scuola darà inoltre ampia diffusione, tramite pubblicazione sul sito, del presente documento di Policy per consentire alle famiglie una piena conoscenza del regolamento sull'utilizzo delle nuove tecnologie.

## 2.1 - IL CURRICOLO DIGITALE

**Nelle Indicazioni Nazionali per il Curricolo della Scuola dell'Infanzia e del Primo Ciclo d'Istruzione del 2012** si legge: *“La diffusione delle tecnologie di informazione e di comunicazione è una grande opportunità e rappresenta la frontiera decisiva per la scuola. Si tratta di una rivoluzione epocale, non riconducibile a un semplice aumento dei mezzi implicati nell'apprendimento. La scuola non ha più il monopolio delle informazioni e dei modi di apprendere. Le discipline e le vaste aree di cerniera tra le discipline sono tutte accessibili ed esplorate in mille forme attraverso risorse in continua evoluzione. Sono chiamati in causa l'organizzazione della memoria, la presenza simultanea di molti e diversi codici, la compresenza di procedure logiche e analogiche, la relazione immediata tra progettazione, operatività, controllo, tra fruizione e produzione. Dunque il “fare scuola” oggi significa mettere in relazione la complessità di modi radicalmente nuovi di apprendimento con un'opera quotidiana di guida, attenta al metodo, ai nuovi media e alla ricerca multi-dimensionale.*

*Al contempo significa curare e consolidare le competenze e i saperi di base, che sono irrinunciabili perché sono le fondamenta per l'uso consapevole del sapere diffuso e perché rendono precocemente effettiva ogni possibilità di apprendimento nel corso della vita. E poiché le relazioni con gli strumenti informatici sono tuttora assai diseguali fra gli studenti come fra gli insegnanti il lavoro di apprendimento e riflessione dei docenti e di attenzione alla diversità di accesso ai nuovi media diventa di decisiva rilevanza.”*

La normativa italiana recepisce la Raccomandazione del Consiglio e il Parlamento Europeo che nel 2006 pubblicano **"Le competenze chiave per l'apprendimento permanente"** in cui si esaminano **otto competenze chiave per l'apprendimento permanente** ritenute essenziali in una società della conoscenza per una cittadinanza attiva, l'inclusione sociale e l'occupazione. La competenza digitale rientra nelle otto competenze chiave del 2006 e confermata nella Raccomandazione del Consiglio del 22 maggio 2018.

*“La competenza digitale presuppone l'interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l'alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l'alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l'essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico.”*

### **Conoscenze, abilità e atteggiamenti essenziali legati a tale competenza**

*“Le persone dovrebbero comprendere in che modo le tecnologie digitali possono essere di aiuto alla comunicazione, alla creatività e all'innovazione, pur nella consapevolezza di quanto ne consegue in termini di opportunità, limiti, effetti e rischi.*

*Dovrebbero comprendere i principi generali, i meccanismi e la logica che sottendono alle tecnologie digitali in evoluzione, oltre a conoscere il funzionamento e l'utilizzo di base di diversi dispositivi, software e reti.*

*Le persone dovrebbero assumere un approccio critico nei confronti della validità, dell'affidabilità e dell'impatto delle informazioni e dei dati resi disponibili con strumenti digitali ed essere consapevoli dei principi etici e legali chiamati in causa con l'utilizzo delle tecnologie digitali."*

*Le persone dovrebbero essere in grado di utilizzare le tecnologie digitali come ausilio per la cittadinanza attiva e l'inclusione sociale, la collaborazione con gli altri e la creatività nel raggiungimento di obiettivi personali, sociali o commerciali.*

*Le abilità comprendono la capacità di utilizzare, accedere a, filtrare, valutare, creare, programmare e condividere contenuti digitali. Le persone dovrebbero essere in grado di gestire e proteggere informazioni, contenuti, dati e identità digitali, oltre a riconoscere software, dispositivi, intelligenza artificiale o robot e interagire efficacemente con essi.*

*Interagire con tecnologie e contenuti digitali presuppone un atteggiamento riflessivo e critico, ma anche improntato alla curiosità, aperto e interessato al futuro della loro evoluzione. Impone anche un approccio etico, sicuro e responsabile all'utilizzo di tali strumenti."*

La competenza digitale è inoltre parte del DigComp 2.2, il Quadro Europeo delle Competenze Digitali per i Cittadini (Digital Competence Framework for Citizens) ovvero l'insieme delle linee guida definite dalla Commissione Europea sulle competenze digitali che i cittadini devono possedere per poter godere di una buona qualità della vita, partecipare alla società democratica ed essere competitivi nel mondo del lavoro.

Su queste indicazioni e in conformità alla L.107/2015, al PNSD e alla normativa vigente l'Istituto Comprensivo prevede nel proprio curriculum azioni per lo sviluppo delle competenze digitali, sia a livello disciplinare sia a livello interdisciplinare.

Le finalità formative delle TIC possono essere sintetizzate nei seguenti punti:

- Favorire la conoscenza dello strumento pc e/o tablet a scopo didattico;
- Sostenere l'alfabetizzazione informatica;
- Favorire la trasversalità delle discipline;
- Facilitare il processo di apprendimento;
- Favorire il processo di inclusione;
- Fornire nuovi strumenti a supporto dell'attività didattica;
- Promuovere situazioni collaborative di lavoro e di studio;
- Sviluppare creatività e capacità di lavorare in gruppo e in modalità sincrona e asincrona;
- Promuovere azioni di cittadinanza attiva;
- Utilizzare in modo critico, consapevole e collaborativo la tecnologia;

Al termine del primo ciclo di istruzione gli studenti dovranno aver maturato le competenze digitali in base alle seguenti dimensioni:

- **Dimensione tecnologica:** questo ambito fa riferimento a una serie di **skills tecnologiche di base**, come ad esempio la conoscenza di dispositivi e programmi per ricercare dati e informazioni.
- **Dimensione cognitiva:** questa dimensione riguarda il saper utilizzare con dimestichezza e spirito critico le Tecnologie della Società dell'Informazione (TSI) per il lavoro, il tempo libero e la comunicazione coadiuvando creatività ed innovazione.
- **Dimensione etica:** il saper interagire con gli altri in modo corretto e responsabile, dalla tutela della privacy al contrasto del fenomeno del cyberbullismo.

## **2.2 - FORMAZIONE DEI DOCENTI SULL'UTILIZZO CONSAPEVOLE E SICURO DI INTERNET E DELLE TECNOLOGIE DIGITALI**

La scuola si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi online. Ciò avverrà tramite specifici momenti di aggiornamento che, con cadenza, verranno organizzati dall'Istituto scolastico con la collaborazione del personale specializzato interno (animatore digitale, referente bullismo e cyberbullismo) e se necessario del personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc...), delle amministrazioni comunali, dei servizi socioeducativi e delle associazioni presenti.

Anche il percorso della formazione specifica dei docenti sull'utilizzo consapevole e sicuro di Internet, può prevedere momenti di autoaggiornamento, momenti di formazione personale o collettiva di carattere permanente, legata all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono sempre di più ed autonomamente anche i ragazzi. Nella sezione collegata alla homepage del sito scolastico <https://www.icsissatreacasali.it/> sarà possibile trovare materiali informativi sulla sicurezza in Internet per l'approfondimento personale, per le attività con gli studenti e gli incontri con i genitori, link a siti specializzati e contributi dal sito "Generazioni connesse".

## **2.3 - IL KIT DIDATTICO**

L'e-Policy prevede, a livello macro, un lavoro di lettura e d'intenti condivisi dall'intera comunità scolastica, a livello micro, invece, immagina che la singola classe lavori anche su tematiche direttamente collegate alla sicurezza in rete, ma complesse e di non immediata ricaduta nelle programmazioni scolastiche (etica e digitale, algoritmi, datafication).

A tal fine si è progettato e predisposto del materiale che possa funzionare sia da attivatore, sia d'accompagnamento ai docenti e agli studenti nella fase più delicata ed incisiva del processo di prevenzione: la lezione in classe.

Pertanto, il progetto Generazioni Connesse, a supporto del lavoro dell'e-Policy ha previsto per i docenti e studenti di ogni segmento scolare un nuovo **Kit Didattico** che contiene materiali per le lezioni e per il proprio aggiornamento, a partire dalla scuola d'infanzia fino alla secondaria di secondo grado. Il Kit può essere usato nella sua interezza oppure può essere oggetto di selezione e scelta, sulla base di quanto fatto dal docente.

### **CAP 3 - GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE ICT (INFORMATION AND COMMUNICATION TECHNOLOGY) DELLA E NELLA SCUOLA**

L'infrastruttura e la strumentazione TIC dell'Istituto sono un bene a disposizione della comunità scolastica e in quanto tale è fatto d'obbligo l'uso corretto e rispettoso delle stesse. I danni causati alle attrezzature saranno a carico di chiunque abbia cagionato il danno. L'accesso ad infrastrutture e strumentazione TIC è riservato ai docenti e agli alunni ed è limitato al perseguimento di scopi formativi.

Il docente accompagnatore è responsabile del corretto uso didattico di hardware e software. Nei laboratori è vietato utilizzare pendrive personali se non dopo opportuno controllo con sistema di antivirus aggiornato.

#### **Accesso ad Internet**

L'accesso ad internet è possibile in tutti i plessi dell'Istituto. L'Istituto è dotato di 2 laboratori informatici in cui sono presenti computer dotati di antivirus, monitorati e tenuti aggiornati dai responsabili dei laboratori informatici. L'accesso alla Rete è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione. Si ribadisce che l'utente è direttamente responsabile, sia civilmente sia penalmente, a norma delle vigenti leggi, per l'uso fatto durante il servizio della rete Internet.

#### **Gestione Accessi**

L'Istituto attualmente è dotato di una rete wireless destinata al solo utilizzo didattico da parte del corpo docente. Tutte le aule sono dotate di pc e la quasi totalità di digital board a disposizione dei docenti sia per la compilazione del registro elettronico sia come supporto alla didattica. Ogni docente accede al registro elettronico attraverso una password personale che non può essere comunicata a terzi. Inoltre, a seguito delle disposizioni introdotte per limitare sempre più la documentazione cartacea nella Pubblica Amministrazione ( DL. n.95/2012 "Disposizioni urgenti per la revisione della spesa pubblica con invarianza dei servizi ai cittadini" -c.d. spending review- Convertito con modificazioni dalla L. 7 agosto 2012, n. 135), tutte le comunicazioni, circolari e disposizioni al personale scolastico sono inviate obbligatoriamente in modalità digitale.

Ugualmente è disposto l'inoltro in via telematica anche per le richieste di permessi e assenze da parte del personale scolastico. Ogni famiglia, infine, riceve le credenziali per l'accesso riservato al registro elettronico, in cui il corpo docente è tenuto a registrare assenze, valutazioni, note e osservazioni.

### **E- Mail**

L'istituto ha un indirizzo ordinario di posta elettronica ordinaria PEO **[pric805003@istruzione.it](mailto:pric805003@istruzione.it)** e un indirizzo di posta elettronica certificata certificato PEC **[pric805003@pec.istruzione.it](mailto:pric805003@pec.istruzione.it)**. Le credenziali sono in possesso del personale amministrativo. La posta elettronica è protetta da antivirus e da antispam.

### **Sito Web della Scuola**

Il sito dell'Istituto Comprensivo è raggiungibile all'indirizzo **<https://www.icsissatrecasali.it/>**. Il Dirigente e lo staff verificano i contenuti destinati alla pubblicazione. Il sito prevede un'area pubblica per le informazioni che non comportano la diffusione di dati personali o riservati, in cui sono reperibili le informazioni sulla vita scolastica, iniziative e scadenze ministeriali, avvisi di carattere generale e un'area riservata accessibile solo dopo autenticazione.

## **3.1 - PROTEZIONE DEI DATI PERSONALI E GDPR**

La protezione dei dati personali delle persone fisiche costituisce un diritto fondamentale. L'art. 8, par. 1, della Carta dei diritti fondamentali dell'Unione europea e l'art. 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

Normativa di riferimento è il Regolamento Generale sulla Protezione dei Dati 2016/679 noto anche come GDPR e il Dlgs 196/2003 con le successive modificazioni e integrazioni.

Il settore dell'istruzione è particolarmente impattato dalla tematica privacy in considerazione del fatto che gli Istituti Scolastici sono chiamati, necessariamente, a trattare un'enorme mole di dati personali.

Con l'entrata in vigore del GDPR è stato introdotto l'obbligo per ciascun Istituto scolastico di provvedere alla designazione di un Responsabile della protezione dei dati personali (RPD o DPO).

I principali obblighi in materia di protezione dei dati personali consistono nella definizione di un "organigramma privacy", nel rilascio dell'informativa al momento della raccolta dei dati e nella tenuta di un registro dei trattamenti.

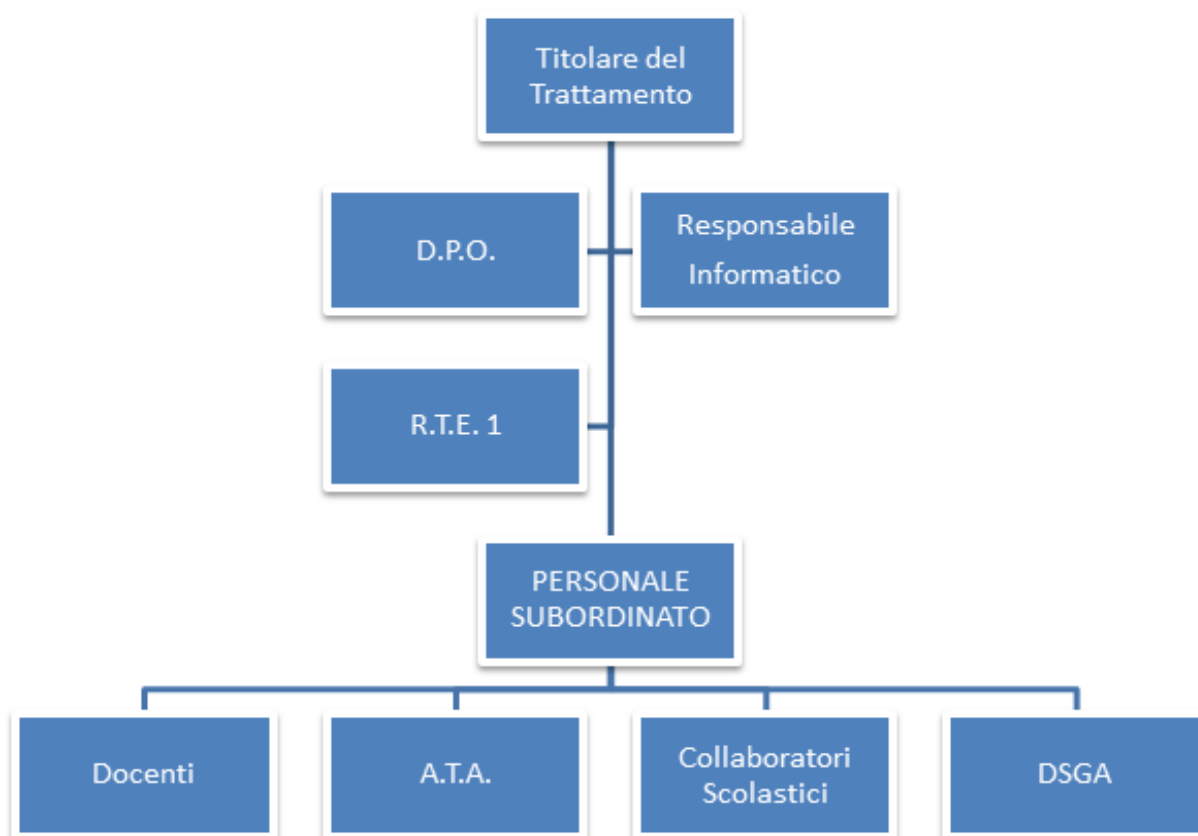
A tal fine l'IC di Sissa Trecasali adotta idonee misure di sicurezza per la protezione dei dati da intrusioni o divulgazioni illecite. I dati verranno trattati solo dal personale incaricato per finalità determinate, esplicite e legittime in base ai principi di pertinenza e non eccedenza.

Il trattamento dei dati personali potrà essere effettuato anche con l'ausilio di strumenti elettronici o comunque automatizzati, con le modalità e le cautele previste dal D. Lgs n.196/2003 e ss.mm.ii.

Alle famiglie viene fornita una informativa sul trattamento dei dati personali ai sensi dell'art. 13 del D. Lgs. n.196/2003 e richiesta un'autorizzazione per l'utilizzo di fotografie, video o altri materiali audiovisivi contenenti l'immagine, il nome e la voce del proprio figlio/a, all'interno di attività educative e didattiche per scopi documentativi, formativi e informativi, durante gli anni di frequenza della Scuola. L'accesso ai dati riportati nel registro elettronico (ritardi, assenze, note e valutazioni) è riservato ai genitori tramite l'invio di una password strettamente personale.

### ORGANIGRAMMA PRIVACY

Riassume e visualizza le differenti figure del Responsabile per la Protezione dei Dati Personali (RPD/DPO), del Titolare del trattamento e soggetti Responsabili ed Autorizzati al trattamento, secondo i ruoli, compiti e responsabilità previsti dalla normativa vigente.



| Legenda                  |                                        |
|--------------------------|----------------------------------------|
| Titolare del Trattamento | Dirigente Scolastico                   |
| D.P.O.                   | Responsabile della Protezione dei dati |
| Responsabile Informatico | Responsabile/Amministratore di Sistemi |
| R.T.I.                   | Responsabile del Trattamento Interno   |
| R.T.E. 1                 | Responsabile del Trattamento Esterno   |

## INFORMATIVA PRIVACY ALUNNI E FAMIGLIE

Il D. Lgs.196/2003 e ss.mm.ii. (Codice in materia di protezione dei dati personali) e del Regolamento Europeo 2016/679 sulla tutela della privacy o GDPR impongono l'osservanza di regole a protezione di tutti i dati personali, sia nella fase del loro trattamento, che della loro diffusione durante l'attività amministrativa e istituzionale.

In ottemperanza a tale normativa il trattamento di tutti i dati personali sarà improntato ai principi di correttezza, liceità, trasparenza e tutela della riservatezza dei diritti degli alunni e delle rispettive famiglie.

## FINALITÀ

I dati personali saranno trattati unicamente per le finalità istituzionali della Scuola, che sono quelle relative all'istruzione ed alla formazione degli alunni e quelle amministrative ad esse strumentali.

## CARATTERE OBBLIGATORIO O FACOLTATIVO DEI DATI PERSONALI

Il conferimento di alcuni dati è obbligatorio in quanto necessario alla realizzazione delle finalità istituzionali. L'eventuale diniego al trattamento di tali dati potrebbe determinare il mancato perfezionamento dell'iscrizione e l'impossibilità di fornire tutti i servizi necessari per garantire il diritto all'istruzione e formazione.

## DATI OBBLIGATORI

I dati personali obbligatori da fornire, strettamente necessari all'esercizio delle funzioni istituzionali, sono, per quanto riguarda l'**allievo**:

- nome e cognome dell'alunno, data e luogo di nascita, codice fiscale, foto, attestati di esito scolastico e altri documenti e/o dati relativi alla carriera scolastica (se proveniente da altra Scuola), permesso di soggiorno (ove necessario).

I dati personali obbligatori da fornire, strettamente necessari all'esercizio delle funzioni istituzionali, sono, per quanto riguarda la **famiglia dell'allievo**:

- nome e cognome dei genitori o di chi esercita la patria potestà, data, luogo di nascita, residenza e domicilio (se diverso dalla residenza) e almeno un recapito telefonico.

I dati personali, qualificati dal Regolamento UE 2016/679 come sensibili e giudiziari, verranno trattati nel rispetto del principio di indispensabilità del trattamento e non saranno soggetti a diffusione, salvo la necessità di comunicare gli stessi ad altri Enti Pubblici (o riceverli da altri Enti Pubblici) nell'esecuzione di attività istituzionali previste da norme di legge in ambito sanitario, previdenziale, tributario, infortunistico, giudiziario. L'acquisizione e il trattamento di questa particolare tipologia di dati avverrà secondo quanto previsto da disposizioni di legge ed in considerazione delle finalità di rilevante interesse pubblico che la Scuola persegue o se indicati nelle Autorizzazioni Generali del Garante per la protezione dei dati.

Di seguito i casi più frequenti:

### Dati idonei a rivelare lo stato di salute dell'alunno o dei familiari:

- Certificazioni legge 104 o certificazioni per DSA;
- Certificazione vaccinale e (in casi particolari) documentazione sanitaria;
- Protocolli di somministrazione farmaci;
- Riammissione a Scuola dopo Certificati medici e dichiarazioni sullo stato di salute o su motivi familiari di natura sensibile (solo ove necessario). Comprese registrazioni su registri o database;
- Ammissione ad esami suppletivi per assenza o impedimento;
- Gestione di infortuni avvenuti a Scuola o nello svolgimento di attività previste dal Ptof;
- Certificazione di esonero da Educazione Fisica o altre certificazioni.

### Dati che potrebbero rivelare orientamento filosofico e religioso:

- Scelta di avvalersi o non avvalersi dell'insegnamento della religione cattolica.

## **DATI FACOLTATIVI**

Per taluni procedimenti amministrativi attivabili soltanto su domanda individuale (ottenimento di particolari servizi, prestazione, benefici, esenzioni, certificazioni, ecc.) può essere necessario il conferimento di ulteriori dati, altrimenti la finalità richiesta non sarebbe raggiungibile. In tali casi verrà fornita un'integrazione verbale della presente informativa.

## **MODALITÀ DI ACQUISIZIONE E DI TRATTAMENTO DEI DATI**

I dati personali dell'alunno e dei familiari vengono acquisiti direttamente dai genitori o dalla Scuola di provenienza nel caso dei trasferimenti. A garanzia dei diritti degli interessati, il trattamento dei dati è svolto secondo le modalità e le cautele previste dalla normativa vigente, seguendo principi di correttezza, di trasparenza, di tutela della dignità e della riservatezza.

Il trattamento può essere svolto in forma cartacea, o attraverso strumenti informatici e telematici, ed i relativi dati saranno conservati, oltre che negli archivi presenti presso la presente istituzione scolastica, anche presso gli archivi del MIUR e suoi organi periferici (Ufficio Scolastico Regionale, Ambito Territoriale Provinciale, ed altri) e presso i database della società fornitrice per la Scuola del servizio di registro elettronico e di altri servizi di segreteria.

I dati, oltre che nel rispetto del D. Lgs.196/2003 e del GDPR, verranno trattati e conservati secondo le regole tecniche di conservazione digitale indicate dall'AGID.

I dati cartacei, invece, secondo quanto previsto dai piani di conservazione e scarto indicati dalla direzione generale degli archivi presso il Ministero dei beni culturali.

Il trattamento prevede come fasi principali: raccolta, registrazione, organizzazione, conservazione, elaborazione, eventuale modifica o aggiornamento, integrazione, comunicazione, diffusione e cancellazione dei dati quando questi cessino di essere necessari.

## **COMUNICAZIONE E DIFFUSIONE DEI DATI**

I soggetti a cui i dati personali potranno essere comunicati nell'ambito della Scuola sono: la Dirigente Scolastica, la DSGA. e i collaboratori della DS. Gli incaricati del trattamento amministrativo, i Docenti del Consiglio di classe, interclasse, intersezione ed i membri dell'equipe per l'integrazione scolastica, relativamente ai dati necessari alle attività didattiche, di valutazione, integrative e istituzionali.

Inoltre potranno essere comunicati dati anche ai collaboratori scolastici ed ai componenti degli organi collegiali, ma solo limitatamente ai dati strettamente necessari alla loro attività.

I dati personali, diversi da quelli sensibili e giudiziari, potranno essere comunicati ad altri Enti Pubblici o privati, esclusivamente nei casi previsti da leggi e regolamenti.

In particolare: altre Amministrazioni del sistema della Pubblica Istruzione, altri Enti pubblici, INAIL, Azienda Sanitaria pubblica competente, Società di Assicurazione per polizza infortuni, Agenzie viaggi, etc.

I soli dati anagrafici potranno essere conferiti a società di trasporto, a strutture pubbliche e private meta di visite scolastiche o oggetto di attività extra e parascolastiche. Potranno essere diffusi esclusivamente i dati previsti dalla normativa e nei casi ivi indicati.

E' consentito, dietro autorizzazione dei genitori all'atto dell'iscrizione, che fotografie e/o video che ritraggono l'alunno/a e/o i suoi familiari durante lo svolgimento di attività scolastiche curriculari ed extracurriculari inserite nel PTOF possano essere utilizzate per fini istituzionali e di documentazione, quali la pubblicazione sul giornalino scolastico, se realizzato, o altre testate giornalistiche locali e nazionali, su poster o manifesti dell'istituto, anche in occasione di partecipazione a fiere e stand dell'orientamento, sul sito web dell'istituto, o sugli altri canali multimediali e social dell'Istituto stesso. In tal caso il trattamento avrà durata temporanea (fino alla permanenza dello studente nella Scuola).

## **TITOLARE DEL TRATTAMENTO DEI DATI**

Il titolare del trattamento dei dati è l'istituzione scolastica stessa, avente personalità giuridica autonoma e legalmente rappresentata dal dirigente scolastico.

## **DIRITTI DELL'INTERESSATO**

Relativamente ai propri dati personali gli interessati potranno esercitare i seguenti diritti: accesso, controllo, modificazione, integrazione e cancellazione garantiti GDPR.

## **DOVERI DELLA SCUOLA**

La Scuola si assume i seguenti doveri:

- Nominare un Dpo;
- Informare immediatamente i diretti interessati e (ove necessario) il garante della privacy e/o la polizia postale nei casi di smarrimento o furto di dati personali;
- Adoperarsi in casi di furto e/o smarrimento per rientrare in possesso dei dati smarriti o sottratti;
- Garantire il diritto all'oblio;
- Migliorare costantemente, in collaborazione con il Dpo, la propria politica di tutela del diritto alla privacy di studenti e famiglie.

## **REGISTRO DELLE ATTIVITA' DI TRATTAMENTO**

Il 24 maggio 2016 è entrato in vigore il Regolamento UE 2016/679 noto anche come GDPR che è diventato direttamente applicabile dal 25 maggio 2018. All'art. 30 del GDPR è stabilito che ogni titolare deve tenere un registro delle attività di trattamento svolte sotto la propria responsabilità che riporti le seguenti informazioni:

- dati di contatto del titolare del trattamento e, dove applicabile, del contitolare del trattamento e del Responsabile della protezione dei dati;
- finalità del trattamento, ossia le finalità per le quali sono trattati tali dati;
- categorie di interessati;
- categorie di dati personali;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Il registro dei trattamenti deve avere forma scritta, anche elettronica è uno strumento fondamentale per disporre di un quadro aggiornato dei trattamenti in essere all'interno dell'Istituto, indispensabile per ogni valutazione e analisi del rischio e va esibito su richiesta al Garante. Secondo il principio di responsabilità, viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati al fine di garantire un'adeguata protezione ed è proprio nel registro dei trattamenti che queste scelte e decisioni sono rese evidenti.

La natura dei dati soggetti al trattamento da parte della Scuola è la seguente:

- Documentazioni complete riguardanti gli alunni, relativi al corso di studi, alla presenza di disabilità, alla certificazione dell'idoneità alla pratica sportiva non agonistica, alla scelta dell'insegnamento della religione cattolica, all'esito di scrutini, esami, piani educativi individualizzati differenziati.
- Documenti prodotti dalle famiglie anche riguardanti la certificazione della situazione patrimoniale e delle condizioni economiche.
- Documentazione riguardante il personale Docente e non Docente anche con elementi di individuazione di appartenenza sindacale, stato di salute, anche di congiunti per i quali vengono richiesti benefici previsti da particolari norme, allo stato di servizio, alla retribuzione, alle eventuali pratiche disciplinari.
- Dati per gestire le negoziazioni e le relative modalità di pagamento per la fornitura di beni e servizi. Dati contabili e fiscali.

### **3.2 - STRUMENTI DI COMUNICAZIONE ONLINE (PUA)**

La Politica d'Uso Accettabile e Responsabile della Rete (P.U.A.) è un documento che racchiude una serie di regole legate all'utilizzo della rete a scuola e a casa da parte di studenti e di tutto il personale (compresi i professionisti esterni che lavorano in contesto scolastico).

#### **UTILIZZO DEI PERSONAL COMPUTER**

##### **A) UTILIZZO DEI PERSONAL COMPUTER DA PARTE DEGLI AMMINISTRATIVI NELLE POSTAZIONI DEGLI UFFICI DI SEGRETERIA**

Il Personal Computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

In particolare:

- L'accesso all'elaboratore deve essere protetto da password che deve essere custodita dall'Amministratore di Sistema con la massima diligenza e non divulgata. La password deve essere attivata per l'accesso alla rete, per lo screensaver e per il software applicativo. Non è consentita l'attivazione della password di accensione (BIOS), senza preventiva autorizzazione da parte dell'Amministratore di Sistema.
- L'Amministratore di Sistema, nell'espletamento delle sue funzioni legate alla sicurezza e alla manutenzione informatica, avrà la facoltà di accedere in qualunque momento anche da remoto (dopo aver richiesto l'autorizzazione all'utente interessato) al personal computer di ciascuno.
- Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. Lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Deve essere attivato su tutti i Personal Computer lo screensaver e la relativa password.
- L'accesso ai dati presenti nel personal computer potrà avvenire quando si rende indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.
- È vietato installare autonomamente programmi informatici salvo autorizzazione esplicita dell'Amministratore di Sistema, in quanto sussiste il grave pericolo di portare Virus informatici o di alterare la stabilità delle applicazioni dell'elaboratore.

- L'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre la struttura a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D. Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.
- È vietato modificare le caratteristiche impostate sul proprio PC, salvo con autorizzazione esplicita dell'Amministratore di Sistema.
- È vietato inserire password locali alle risorse informatiche assegnate (come ad esempio password che non rendano accessibile il computer agli amministratori di rete), se non espressamente autorizzati e debitamente comunicate all'Amministratore di Sistema.
- È vietata l'installazione sul proprio PC di dispositivi di memorizzazione, comunicazione o altro (come ad esempio pendrive, dischi esterni, smartphone, ecc.), se non con l'autorizzazione espressa dell'Amministratore di Sistema. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'Amministratore di Sistema nel caso in cui vengano rilevati virus o eventuali malfunzionamenti.

## **B) UTILIZZO DEI PERSONAL COMPUTER DA PARTE DEL PERSONALE DOCENTE NELLE POSTAZIONI DEDICATE E NEI LABORATORI DI INFORMATICA**

Le apparecchiature presenti nella Scuola sono Patrimonio Comune e vanno utilizzate con rispetto. I PC presenti in aula professori nei Plessi della Scuola Secondaria e quelli disponibili per i Docenti nei Plessi della Scuola Primaria e dell'Infanzia devono essere dotati di password e devono avere un account utente e un account amministratore. La password dell'account amministratore deve essere conosciuta solo dal responsabile informatico del Plesso e dalle Funzioni Strumentali per le nuove tecnologie per evitare che tutti possano installare software a piacimento.

Il computer dell'aula insegnanti, salvo esplicito mandato da parte di un Docente, deve essere usato dai soli Docenti e non dal personale di servizio. Il PC viene utilizzato:

- per accedere al Registro Elettronico nel caso non sia stato possibile farlo in classe per problematiche legate alla connessione;
- per archiviare file utili ai Docenti (es. modulistica varia);
- per accedere alle comunicazioni presenti nella bacheca del Registro e nel sito della Scuola;
- per elaborare materiale didattico.

Non devono essere salvati sui PC messi a disposizione dei Docenti, i file contenenti dati degli alunni (voti, fasce di livello, note disciplinari, elenchi con dati anagrafici o numeri di telefono delle famiglie) e altri file personali degli insegnanti non inerenti l'attività lavorativa.

Non devono essere modificate le impostazioni, né possono essere installati software salvo autorizzazione esplicita del Referente per l'informatica e della Funzione strumentale, in quanto sussiste il grave pericolo di portare virus informatici o di alterare la stabilità delle applicazioni dell'elaboratore. L'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre la struttura a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D. Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

È vietata l'installazione sui PC di dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, pendrive, dischi esterni, telefoni, ecc.), se non con l'autorizzazione espressa del responsabile per l'informatica del Plesso e delle Funzioni Strumentali per le nuove tecnologie. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente i suddetti responsabili caso in cui vengano rilevati virus o eventuali malfunzionamenti. Per il trasferimento di file devono essere utilizzati servizi di archiviazione online (gratuiti) quali Google Drive o altri, in modo da non incorrere nel rischio virus.

### **C) DISPOSIZIONI SULL'USO DEL LABORATORIO DI INFORMATICA**

Gli alunni devono essere sempre accompagnati da un insegnante che sarà garante e direttamente responsabile dell'utilizzo del Laboratorio nel rispetto del regolamento di Istituto. Durante le ore di utilizzo del Laboratorio gli alunni devono lasciare le cartelle in classe, portando con sé lo stretto necessario.

Il Docente che utilizza il Laboratorio con la propria classe è tenuto a informare gli studenti sulle disposizioni in materia di sicurezza e sui rischi a cui vengono esposti durante le attività.

Quando un insegnante, da solo o con la classe, usufruisce del Laboratorio deve obbligatoriamente registrare il proprio nome e l'eventuale classe, nell'apposito registro delle presenze di Laboratorio, l'orario di ingresso e quello di uscita.

Per quanto riguarda la Scuola Secondaria di primo grado l'insegnante è tenuto a compilare in ogni sua parte il modulo di assegnazione postazioni presente in Laboratorio.

Ogni inconveniente hardware o software deve essere tempestivamente segnalato al responsabile del Laboratorio che lo comunicherà altrettanto tempestivamente alle Funzioni Strumentali per le nuove tecnologie.

È compito specifico del preposto garantire il buon funzionamento dei sistemi presenti nel Laboratorio stesso e la gestione del materiale di consumo, delle richieste di assistenza tecnica, della conservazione dei software.

Al di fuori del normale orario di utilizzo il Laboratorio deve rimanere chiuso a chiave.

Nei Laboratori è vietato utilizzare chiavette USB.

È vietato cancellare o alterare file e dati presenti in hard-disk; non devono inoltre essere variate le proprietà dello schermo.

La stampa dei file didattici dei ragazzi viene eseguita sotto il controllo dell'insegnante. Non sono consentite stampe di documenti personali. Le stampe dovranno essere registrate in apposito modulo presente nel Laboratorio.

All'uscita dal Laboratorio si dovrà lasciare il mobilio in ordine, le macchine spente correttamente, tastiera e mouse al loro posto, videoproiettore spento correttamente onde evitare danni alla lampada e allo stesso. Prima di chiudere il Laboratorio l'interruttore generale deve essere spento salvo indicazioni contrarie.

## **E) USO DEI SOFTWARE**

I software installati sono a esclusivo uso didattico.

È fatto divieto di usare software non conformi alle leggi sul copyright. Gli insegnanti possono installare un nuovo software sui PC del Laboratorio previa autorizzazione del Referente per l'informatica e delle Funzioni Strumentali per le nuove tecnologie.

## **ACCESSO A INTERNET NEI LABORATORI**

L'accesso a Internet è consentito al personale Docente e non Docente solo a esclusivo uso didattico e/o di formazione e alle classi accompagnate esclusivamente sotto la responsabilità di un insegnante.

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.

È vietato inserire sui PC connessi in rete programmi contenenti virus, scaricare da Internet software non autorizzati, installare software senza licenza, scaricare per stampare in Laboratorio materiale a uso personale.

## **UTILIZZO DELLE DIGITAL BOARD PRESENTI NELLE AULE**

L'uso delle Digital Board e delle annesse dotazioni del kit è riservato ai Docenti della classe in cui la Digital Board è inserita.

L'uso da parte degli alunni è consentito esclusivamente per scopi didattici e sempre con la guida e alla presenza di un Docente.

Se vengono rilevati malfunzionamenti si relaziona quanto prima alle Funzioni Strumentali per le nuove tecnologie, preferibilmente tramite mail tramite mail.

Mettere in STANDBY la Digital Board durante i momenti in cui non viene utilizzata e SPEGNERE correttamente a fine giornata lavorativa, verificare la presenza di tutti i materiali (penna, telecomando, ecc.) e porli in luogo sicuro.

Ogni Docente è tenuto a verificare all'inizio della sua sessione di lavoro che le attrezzature da utilizzare siano funzionanti e in ordine e, se si riscontrassero dei problemi, questi devono essere subito comunicati al Referente.

Il Docente deve verificare al termine della lezione che tutte le apparecchiature siano spente e che tutti gli accessori siano stati adeguatamente ricollocati.

È fatto divieto assoluto agli alunni l'uso della Digital Board senza la presenza di un Docente.

Alla fine delle proprie lezioni il Docente deve spegnere il computer (o metterlo in blocco) per evitare che venga impropriamente usato dai ragazzi nel cambio di insegnante o durante l'intervallo. Se l'insegnante per qualsiasi motivo abbandona l'aula deve mettere in blocco la Digital Board e chiamare un collaboratore scolastico.

Si deve controllare sempre che l'antivirus sia aggiornato ed evitare l'inserimento di chiavette USB portate dagli alunni. Al posto delle chiavette USB è preferibile usare servizi online di archiviazione dati.

Gli alunni che utilizzano impropriamente le Digital Board e/o per negligenza le danneggiano ricevono una sanzione disciplinare e sono tenuti a rimborsare il danno.

Tutti i file prodotti con la Digital Board devono essere salvati dal Docente interessato utilizzando servizi online di archiviazione dati e non lasciati “sparsi” sul desktop. A proposito di questo salvataggio, si ricorda che prima dell’inizio di ogni anno scolastico i PC e le Digital Board devono essere “ripuliti” dai vecchi file non più necessari e dal software non necessario.

## **UTILIZZO DELLA RETE INFORMATICA**

Le unità di rete sono aree di condivisione di informazioni strettamente professionali sulle quali vengono svolte regolari attività di controllo, amministrazione e backup e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all’attività lavorativa non può essere dislocato in queste unità, nemmeno per brevi periodi. Si parte quindi dal presupposto che i file relativi alla produttività individuale vengono salvati sul server e i limiti di accesso sono regolarizzati da apposite policies di sicurezza che suddividono gli accessi tra gruppi e utenti.

L’amministratore di Sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza o in violazione del presente regolamento sia sui PC degli incaricati sia sulle unità di rete. Le password d’ingresso alla rete e ai programmi sono segrete e non vanno comunicate a terzi.

Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È, infatti, assolutamente da evitare un’archiviazione ridondante.

È importante togliere tutte le condivisioni dei dischi o di altri supporti configurate nel Personal Computer se non strettamente necessarie (e per breve tempo) allo scambio dei file con altri colleghi. Esse sono infatti un ottimo “aiuto” per i software che cercano di “minare” la sicurezza dell’intero sistema. Sarà compito dell’Amministratore di Sistema provvedere alla creazione di un’area condivisa sul server per lo scambio dei dati tra i vari utenti.

Nell’utilizzo della Rete informatica è fatto divieto di:

- Utilizzare la Rete in modo difforme da quanto previsto dal presente regolamento;
- Conseguire l’accesso non autorizzato a risorse di rete interne ed esterne alla Rete comunale;
- Agire deliberatamente con attività che influenzano negativamente la regolare operatività della Rete e ne restringono l’utilizzabilità e le prestazioni per altri utenti;
- Effettuare trasferimenti non autorizzati di informazioni (software, dati, ecc);
- Installare componenti hardware non compatibili con l’attività istituzionale;
- Rimuovere, danneggiare o asportare componenti hardware;
- Utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare file e software di altri utenti;

- Utilizzare software visualizzatori di pacchetti TCP/IP (sniffer), software di decodifica password (cracker) e più in generale software rivolti alla violazione della sicurezza del sistema e della privacy;
- Usare l'anonimato o servirsi di risorse che consentano di restare anonimi.

## **UTILIZZO DI INTERNET**

I Personal Computer, qualora abilitati alla navigazione in Internet, costituiscono uno strumento necessario allo svolgimento della propria attività lavorativa. Nell'uso di Internet e della Posta Elettronica non sono consentite le seguenti attività:

- L'uso di Internet per motivi personali;
- L'accesso a siti inappropriati (esempio siti pornografici, di intrattenimento, ecc.);
- Lo scaricamento (download) di software e di file non necessari all'attività istituzionale;
- Utilizzare programmi per la condivisione e lo scambio di file in modalità peer to peer (Napster, Emule, BitTorrent, uTorrent, ecc.);
- Accedere a flussi in streaming audio/video da Internet per scopi non istituzionali (ad esempio ascoltare la radio o guardare video o filmati utilizzando le risorse Internet);
- Un uso che possa in qualche modo recare qualsiasi danno all'Istituto o a terzi.

## **UTILIZZO DELLA POSTA ELETTRONICA**

La casella di posta, assegnata dall'Istituto, è uno strumento di lavoro.

Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica della struttura per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione.

È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali con l'istituto ricevuta da personale non autorizzato, deve essere visionata ed inoltrata al DSGA, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.

La documentazione elettronica che viene contraddistinta da diciture od avvertenze dirette ad evidenziare il carattere riservato o segreto, non può essere comunicata all'esterno senza preventiva autorizzazione del Responsabile del trattamento.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.

Per la trasmissione di file all'interno della struttura è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati. È obbligatorio controllare i file Attachments di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web, HTTP o FTP non conosciuti) e accertarsi dell'identità del mittente.

In particolare nell'uso della Posta Elettronica non sono consentite le seguenti attività:

La trasmissione a mezzo di posta elettronica di dati sensibili, confidenziali e personali di alcun genere, salvo i casi espressamente previsti dalla normativa vigente in materia di protezione dei dati personali (D.lgs. 196 del 30/6/2003).

- L'apertura di allegati ai messaggi di posta elettronica senza il previo accertamento dell'identità del mittente.
- Inviare tramite posta elettronica user-id, password, configurazioni della rete interna, indirizzi e nomi dei sistemi informatici.

## **UTILIZZO DEI SUPPORTI MAGNETICI**

Tutti i supporti magnetici riutilizzabili (hard disk, memorie USB, CD riscrivibili) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione. I supporti magnetici contenenti dati sensibili e giudiziari devono essere custoditi in archivi chiusi a chiave.

Tutti i supporti magnetici riutilizzabili obsoleti devono essere consegnati all'Amministratore di Sistema per l'opportuna distruzione. Ogni qualvolta si procederà alla dismissione di un Personal Computer l'Amministratore di Sistema provvederà alla distruzione delle unità di memoria interne alla macchina stessa (hard-disk, memorie solide).

## **UTILIZZO DI PC PORTATILI**

L'utente è responsabile del PC portatile assegnatogli che deve custodire con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro. Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna. I PC portatili utilizzati all'esterno (convegni, riunioni fuori sede, ecc.), in caso di allontanamento devono essere custoditi in un luogo protetto.

## UTILIZZO TABLET PER USO DIDATTICO

Ai Tablet si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

Ogni Tablet ha un numero di inventario posto sia sul dispositivo sia sulla scatola che lo contiene.

Il Tablet affidato al personale è custodito in apposito armadio nell'aula informatica o in altro luogo sicuro.

I collaboratori scolastici apriranno l'aula e l'armadio e ogni insegnante, all'inizio delle lezioni, prenderà il Tablet e il cavo di alimentazione relativo alla propria classe.

I Tablet possono essere utilizzati per:

- accedere al Registro Elettronico, nel caso non sia stato possibile farlo con il Pc della classe per problematiche tecniche;
- archiviare file utili ai Docenti (es. modulistica varia);
- per accedere alle comunicazioni presenti nella bacheca del Registro e nel sito della Scuola;
- per elaborare materiale didattico.

Al termine della propria lezione l'insegnante avrà cura di fare il logout lasciando comunque acceso il dispositivo nel caso in cui debba essere usato dal/la collega dell'ora successiva.

Non è consentita l'installazione di applicazioni se non dopo richiesta al responsabile dei Laboratori informatici ed unicamente provenienti da Google Play.

Non è consentito portare il Tablet fuori dall'Istituto.

Il Tablet per nessun motivo va lasciato incustodito. Nel caso in cui si debba uscire, per qualche motivo, dall'aula o nel caso in cui ci si debba spostare in aule speciali o in palestra, si avrà cura di portarlo dietro.

In caso di evacuazione, il Docente deve portare con sé il Tablet.

Alla fine delle lezioni il dispositivo deve essere spento e riportato, insieme al cavo d'alimentazione, in aula informatica (o altro luogo preposto) dove sarà rimesso, all'interno della propria confezione, in armadio/cassaforte.

È responsabile del Tablet l'insegnante, curricolare e di sostegno, che in quell'ora è incaricato a essere in classe sia per ragioni di orario, sia perché supplente.

Segnalare immediatamente alle Funzioni Strumentali per le nuove tecnologie eventuali anomalie nel funzionamento dei dispositivi, per poter procedere subito alla risoluzione dei problemi.

## UTILIZZO DELLE STAMPANTI E DEI MATERIALI DI CONSUMO

L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner) è riservato esclusivamente ai compiti di natura strettamente istituzionale. Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi. È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

### 3.3 – Strumentazione personale - BYOD

Il PNSD (legge 107/2015) prevede diverse azioni mirate all'innovazione tecnologica e culturale della scuola.

L'azione 6 riguarda concretamente il così detto BYOD (bringyourowndevice) definito come l'insieme delle azioni che promuovono l'utilizzo e l'integrazione di dispositivi personali nelle attività didattiche. Questa possibilità dovrà anche prevedere soluzioni che garantiscono la sicurezza e l'educazione alla sicurezza digitale che “permettano a tutti gli studenti e docenti della scuola di utilizzare un dispositivo, anche proprio.”

In seguito all'elaborazione del PNSD il MIUR ha elaborato un decalogo del BYOD dove enumera i dieci punti fondamentali da tenere in considerazione:

1. Ogni novità comporta cambiamenti. – Ogni cambiamento deve servire per migliorare l'apprendimento e il benessere delle studentesse e degli studenti e più in generale dell'intera comunità scolastica.
2. I cambiamenti non vanno rifiutati, ma compresi e utilizzati per il raggiungimento dei propri scopi. - insegnare a usare bene e integrare nella didattica quotidiana i dispositivi, anche attraverso una loro regolamentazione. Proibire l'uso dei dispositivi a scuola non è la soluzione. A questo proposito ogni scuola adotta una Politica di Uso Accettabile (PUA) delle tecnologie digitali.
3. La scuola promuove le condizioni strutturali per l'uso delle tecnologie digitali. - Fornisce, per quanto possibile, i necessari servizi e l'indispensabile connettività, favorendo un uso responsabile - dei dispositivi personali (BYOD).
4. La scuola accoglie e promuove lo sviluppo del digitale nella didattica. - La presenza delle tecnologie digitali costituisce una sfida e un'opportunità per la didattica e per la cultura scolastica.
5. I dispositivi devono essere un mezzo, non un fine. - È la didattica che guida l'uso competente e responsabile dei dispositivi.

6. L'uso dei dispositivi promuove l'autonomia delle studentesse e degli studenti. - È in atto una graduale transizione verso situazioni di apprendimento che valorizzano lo spirito d'iniziativa e la responsabilità di studentesse e gli studenti. Bisogna sostenere un approccio consapevole al digitale nonché la capacità d'uso critico delle fonti di informazione, anche in vista di un apprendimento lungo tutto l'arco della vita.
7. Il digitale nella didattica è una scelta: sta ai docenti introdurla e condurla in classe. - L'uso dei dispositivi in aula è promosso dai docenti, nei modi e nei tempi che ritengono più opportuni.
8. Il digitale trasforma gli ambienti di apprendimento. - Le possibilità di apprendere sono ampliate (...), occorre regolamentare le modalità e i tempi dell'uso e del non uso, anche per imparare a riconoscere e a mantenere separate le dimensioni del privato e del pubblico.
9. Rafforzare la comunità scolastica e l'alleanza educativa con le famiglie. - È necessario che l'alleanza educativa tra scuola e famiglia si estenda alle questioni relative all'uso dei dispositivi personali. (...) Lo scopo condiviso è promuovere la crescita di cittadini autonomi e responsabili.
10. Educare alla cittadinanza digitale è un dovere per la scuola. - Formare i futuri cittadini della società della conoscenza significa educare alla partecipazione responsabile, all'uso critico delle tecnologie, alla consapevolezza e alla costruzione delle proprie competenze in un mondo sempre più connesso.

In data 19.12.2022 con prot. 7190 il MIM pubblica una Nota firmata dal Ministro dell'Istruzione e del Merito Giuseppe Valditara, contenente le indicazioni sull'utilizzo dei telefoni cellulari e di analoghi dispositivi elettronici nelle classi. Vigé in via generale un divieto di utilizzo in classe di telefoni cellulari. L'utilizzo dei cellulari e di altri dispositivi elettronici può essere ovviamente consentito, su autorizzazione del docente, e in conformità con i regolamenti di istituto, per finalità didattiche, inclusive e formative, anche nell'ambito degli obiettivi del Piano Nazionale Scuola Digitale (PNSD) e della "cittadinanza digitale".

Tanto premesso l'Istituto Comprensivo di Sissa Trecasali, in linea con il Piano Nazionale Scuola Digitale che promuove con l'azione #6 un'apertura al BYOD (Bring Your Own Device- "porta il tuo dispositivo"), consente agli alunni l'uso di smartphone, tablet e altri dispositivi mobili **solo su indicazioni dei docenti, con esclusiva finalità didattica, in momenti ben definiti e con modalità prescritte dall'insegnante.** Gli insegnanti di classe avranno cura di vigilare sul corretto utilizzo di tali dispositivi.

Agli alunni non è consentito:

- a) usare Internet per scopi diversi da quelli didattici;
- b) scaricare musica, video e programmi da internet o qualsiasi file senza il consenso dell'insegnante;
- d) accedere ai Social Network (Facebook, Instagram...);

e) Giochi e console, tra cui la Sony Playstation, Microsoft Xbox e similari, che possono avere accesso a Internet non filtrato, non sono consentiti. Saranno requisiti dal docente che ravvisa l'infrazione e consegnati al genitore convocato, che sarà contestualmente informato dell'eventuale sanzione disciplinare comminata al trasgressore.

### **Gli strumenti personali per docenti**

Durante l'orario di lezione è consentito ai docenti l'uso di dispositivi elettronici personali a scopo didattico e a integrazione dei dispositivi scolastici disponibili (es. il computer di classe). Non è possibile utilizzare cellulari e smartphone per attività personali e che esulino dall'insegnamento.

### **Per il personale della scuola**

Durante l'orario di servizio è consentito al personale scolastico l'uso di cellulari e smartphone per comunicazioni personali urgenti. L'uso di altri dispositivi elettronici personali o dell'istituto è consentito solo per attività funzionali al servizio.

## **CAP 4 - RISCHI ONLINE: CONOSCERE, PREVENIRE E RILEVARE**

### **Il rischio online si configura come la possibilità per il minore di:**

- commettere azioni online che possano danneggiare se stessi o altri;
- essere una vittima di queste azioni;
- osservare altri commettere queste azioni.

È importante riconoscere questi fenomeni e saperli distinguere tra loro in modo da poter poi adottare le strategie migliori per arginarli e contenerli, ma è altrettanto importante conoscere le strategie da mettere in campo per permettere una riduzione dei fattori di rischio.

### **4.1 - STRATEGIE DI INTERVENTO**

Gli strumenti da adottare per poter ridurre l'incidenza di situazioni di rischio si configurano come interventi di **sensibilizzazione e prevenzione**.

Nel caso della **sensibilizzazione** si tratta di azioni che hanno come obiettivo quello di innescare e promuovere un cambiamento; l'intervento dovrebbe fornire non solo le informazioni necessarie (utili a conoscere il fenomeno), ma anche illustrare le possibili soluzioni o i comportamenti da adottare.

**La Sensibilizzazione** implica azioni indirette basate sull'acquisizione da parte degli alunni delle **life skills** quali:

- **Capacità di risolvere problemi (Problem solving);**
- **Capacità di prendere decisioni (Decision making);**
- **Creatività;**
- **Senso critico;**
- **Comunicazione efficace;**
- **Capacità di relazionarsi con gli altri;**
- **Autocoscienza;**
- **Empatia;**
- **Gestione delle emozioni;**
- **Gestione dello stress**

Al personale che opera nella scuola, e in modo particolare agli insegnanti, viene oggi offerta la possibilità di essere promotori e garanti della costruzione dialogica di un percorso formativo partecipato.

Nel caso della **prevenzione** si tratta di un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale e quindi ridurre i rischi per la sicurezza di bambine/i e ragazze/i.

A tal fine l'Istituto intende mettere in campo azioni per rispondere ai bisogni dell'utenza, attraverso una risposta integrata con la rete dei servizi territoriali locali (tra cui ASP, Polizia postale, etc.).

Creare momenti "ad hoc", quali gli "sportelli", "incontri - dibattiti" con i rappresentanti della Polizia, avvocati, studenti etc. Una buona prevenzione è anche affinare l'**Osservazione dei Campanelli di Allarme ed essere in grado di valutare Rischi e Azioni.**

| RISCHI                                                                                                                             | AZIONI                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Accesso a contenuti inopportuni di qualsiasi genere attraverso motori di ricerca via Internet.</b>                              | Dotare i dispositivi della scuola di filtri che impediscano l'accesso a siti web non adatti ai minori (black list).                                                                                                                                                                  |
| <b>Violazione della Privacy.</b><br><br><b>Smarrimento password personale o sospetto furto identità per accrediti di Istituto.</b> | Dare informativa sulla tutela della privacy e richiedere consenso per trattamento dei dati personali a fini didattici.<br><br>In caso di violazione il Dirigente Scolastico deve esserne informato in quanto a seconda dell'illecito sono previste sanzioni amministrative o penali. |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <p>Blocco utenza e resettaggio o cancellazione/rinnovo dell'utenza interessata.</p> <p>Formazione continua al mantenimento in sicurezza del proprio account.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Adescamento online (grooming)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <p>Sensibilizzazione sull'esistenza di adulti che tentano di avvicinare minorenni al fine di instaurare una relazione intima o sessualizzata.</p> <p>Qualora si venga a conoscenza di casi simili, occorre valutarne la fondatezza e avvisare il Dirigente Scolastico per l'intervento delle forze dell'ordine.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <p><b>Cyberbullismo:</b></p> <p><b>Flaming:</b> litigi on line nei quali si fa uso di un linguaggio violento e volgare.</p> <p><b>Harassment:</b> Molestie. Invio ripetuto di messaggi offensivi, scortesi e insultanti.</p> <p><b>Cyberstalking:</b> Cyber-persecuzione. Invio ripetuto di messaggi contenenti minacce fortemente intimidatori al punto che la vittima arriva a temere per la propria incolumità.</p> <p><b>Denigration:</b> “Sparlare” di qualcuno online. Inviare o pubblicare pettegolezzi e dicerie denigratori su una persona per danneggiarne la reputazione e / o le amicizie.</p> <p><b>Impersonation.</b> Sostituzione di persona. Violare l'account di qualcuno. con l'obiettivo di inviare dal medesimo messaggi ingiuriosi che screditino la vittima.</p> <p><b>Outing estorto.</b> Registrazione di confidenze, raccolte all'interno di un ambiente privato, in</p> | <p>Formazione continua, campagne di sensibilizzazione e informazione attraverso laboratori o conferenze rivolti a tutte le componenti della comunità scolastica.</p> <p>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.</p> <p>Occorre confrontarsi con Referente e con il Dirigente Scolastico sulle azioni da intraprendere.</p> <p>È necessario monitorare i comportamenti suscettibili di attenzione attraverso <b>il diario di bordo (All.1)</b></p> <p>Diffusione del <b>Manifesto della Comunicazione Non Ostile</b> il cui scopo è ridefinire e riflettere sullo stile con cui stiamo in rete e comunichiamo, ricordandoci che le parole sono importanti e vanno scelte con cura. <b>(All. 6)</b></p> |

|                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>un clima di fiducia per poi inserirle integralmente in un blog pubblico.</p> <p><b>Esclusione:</b> estromissione intenzionale dalla attività on line.</p> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <p><b>Navigazione in siti inadeguati, dediti all'hate speech.</b></p> <p><b>Uso videogiochi diseducativi e violenti.</b></p>                                 | <p>Occorre convocare i genitori per richiamarli a un maggiore controllo sulla fruizione di Internet da parte dei propri figli.</p> <p>Proporre in ambito scolastico attività di analisi e riflessione in modo da <b>fornire agli studenti gli strumenti necessari per combattere gli stereotipi su cui spesso si fondano forme di <u>hate speech</u>, (legati spesso alla razza, al genere, all'orientamento sessuale, alla disabilità)</b></p> <p>Diffusione della campagna di sensibilizzazione <b><u>“No Hate Speech Movement”</u></b> avviato dal Consiglio d’Europa con l’obiettivo di combattere il razzismo e la discriminazione mediante l’adozione di comportamenti che contrastino ogni forma di violenza e odio.</p> |
| <p><b>Sexting e pedopornografia</b></p>                                                                                                                      | <p>La <b>pedopornografia online è un reato</b> (art. 600-ter comma 3 del c.p.) che consiste nel produrre, divulgare, diffondere e pubblicizzare, immagini o video ritraenti persone minorenni coinvolte in comportamenti sessualmente espliciti, concrete o simulate o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.</p> <p>Avvisare tempestivamente il Dirigente Scolastico per l'intervento delle forze dell'ordine.</p> <p>Inserimento nel curriculum di temi legati all'educazione all'affettività/Ed civica in ottica preventiva.</p>                                                                                                                                                      |

|                                                     |                                                                   |
|-----------------------------------------------------|-------------------------------------------------------------------|
| <b>Accesso ad informazioni scorrette; Fake news</b> | <b>Diffusione del Decalogo: "Fake News- Basta Bufale" (All.7)</b> |
|-----------------------------------------------------|-------------------------------------------------------------------|

**Cyberbullismo:** è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un “pubblico”? Tra coetanei? In modo ripetuto e intenzionale? C’è un danno percepito alla vittima? etc.). È necessario poi valutare l’eventuale stato di disagio vissuto dagli/lle studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).

**Adescamento online:** se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenni e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all’adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l’attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l’ausilio di una persona esperta in psicologia o psichiatria infantile.

**Sexting:** nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l’obiettivo primario di tutelare il minore e ottenere, per quanto possibile, la rimozione del materiale on-line e il blocco della sua diffusione per mezzo dei dispositivi mobili.

**Hate speech:** Il fenomeno di “incitamento all’odio” o “discorso d’odio”, indica discorsi (post, immagini, commenti etc.) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona (identificate come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena. Più ampiamente il termine “hate speech” indica un’offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, eccetera) ai danni di una persona o di un gruppo.

**Tale fenomeno, purtroppo, è sempre più diffuso ed estremamente importante affrontarlo anche a livello educativo e scolastico con l’obiettivo di:**

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all’orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l’impegno, anche attraverso i media digitali e i social network;
- favorire una presa di parola consapevole e costruttiva da parte dei giovani.

Occorre valorizzare la dimensione relazionale dei più giovani, sensibilizzandoli verso capacità di analisi e, quindi, discernimento, per fornire strumenti idonei tanto comunicativi quanto educativi sotto l'aspetto civico e morale.

La corresponsabilità con la famiglia è un precursore fondamentale nell'azione didattico-educativa della scuola, anche per attivare progettazioni complementari con finalità socio-educative.

Per i reati più gravi e urgenti (si pensi all'importanza, in una situazione di cyberbullismo, che un contenuto denigratorio venga tempestivamente bloccato) ci si può avvalere della:

- **Polizia Postale e delle Comunicazioni:** accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico:** segnala all'Autorità Giudiziaria e ai Servizi Sociali e competenti. **Il Modello** per chiedere l'intervento del Garante per la protezione dei dati personali e segnalare episodi di bullismo sul web o sui social network da inviare a [cyberbullismo@gpdp.it](mailto:cyberbullismo@gpdp.it) è contenuto nell'**Allegato 4**.
- **Tribunale per i Minorenni:** segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza.
- Per quanto riguarda la necessità di segnalazione e rimozione di contenuti online lesivi, ciascun minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità del minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella Rete.
- Se entro 24 ore il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.
- Per una mappatura degli indirizzi di tali strutture sul territorio nazionale è possibile consultare il **Vademecum di Generazioni Connesse** "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani", senza dimenticare che la Helpline di Telefono Azzurro è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso.

Inoltre sono attivi due servizi messi a disposizione dal **Safer Internet Center**:

- **Clicca e segnala** di Telefono Azzurro [www.azzurro.it/it/clicca-e-segnala](http://www.azzurro.it/it/clicca-e-segnala)
- **Stop-it** di Save the Children [www.stop-it.it](http://www.stop-it.it)

- **La Helpline di Telefono Azzurro** che comprende sia **la linea di ascolto 1.96.96, attiva 24 ore al giorno, 365 giorni all'anno** sia la **chat, attiva dal lunedì al venerdì (8-22) e sabato/domenica (8-20)**. **Il servizio Helpline è riservato, gratuito e sicuro** ed è dedicato ai giovani o ai loro familiari. Una volta ricevuta la segnalazione gli operatori procederanno a coinvolgere le autorità competenti in materia.

## **4.2 - LA RILEVAZIONE**

La rilevazione dei casi è compito dell'intera comunità educante. Sono da segnalare tutte quelle situazioni che si configurano come episodi di cyberbullismo, violazione della privacy, uso inappropriato della rete mediante il ricorso a procedure chiare e che includano la collaborazione dei servizi locali (in primis le ASL e la Polizia Postale).

## **4.3- SEGNALEAZIONE E GESTIONE DEI CASI**

Questa sezione dell'ePolicy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse (vedi allegati a seguire).

Alunni, famiglie, docenti e tutto il personale scolastico attivo nell'Istituto si impegnano a segnalare al Dirigente Scolastico i casi di bullismo e cyberbullismo di cui sono a conoscenza, anche se presunti, in modo da attivare tutte le procedure di verifica necessarie all'individuazione del bullo, della vittima e delle dinamiche intercorse tra i due.

Per le segnalazioni di fatti rilevati sono previsti i seguenti strumenti che i docenti possono utilizzare sulla base della gravità dell'accaduto:

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

Nell'effettuare la segnalazione è consigliabile dotarsi di un **modulo** così da esporre in forma chiara e sintetica tutte le informazioni necessarie alla presa in carico della situazione. **(All.2)**

Inoltre è necessario per tenere traccia di ciò che è avvenuto e di come è stato gestito tramite un **diario di bordo (All.1)**

Si rammenta che l'insegnante riveste la qualifica di pubblico ufficiale (ex [art. 357 c.p.](#)) in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative.

Il Codice Penale Italiano, all'[art. 357](#), definisce il pubblico ufficiale come colui che esercita una “pubblica funzione legislativa, giudiziaria o amministrativa”. Questa definizione si estende ai docenti nel momento in cui sono impegnati nell’esercizio delle loro funzioni all’interno degli istituti scolastici.

La Corte di Cassazione, con la sentenza [n. 15367/2014](#), ha ribadito la qualifica di pubblico ufficiale per l’insegnante, estendendo tale riconoscimento non solo alla tenuta delle lezioni, ma anche a tutte le attività connesse. Questo include, ad esempio, gli incontri con i genitori degli allievi.

Le situazioni problematiche in relazione all’uso delle tecnologie digitali dovrebbero essere sempre gestite da un team di docenti composto da:

1. Dirigente
2. Docente referente
3. L’animatore digitale (secondo il Piano Nazionale per la Scuola Digitale, abbreviato in PNSD, introdotto dalla Legge 107/2015)
4. Referente bullismo (ex. Legge Italiana Contro il Cyberbullismo, l. 71/2017) e Team Bullismo e Cyberbullismo
5. Altri docenti già impegnati nelle attività di promozione dell’educazione civica.

Le situazioni di pregiudizio presunto o reale possono richiedere il supporto e l'intervento di esperti esterni alla scuola.

**Come descritto nelle procedure di questa sezione, si potrebbero palesare due macro - casi:**

**CASO A (SOSPETTO)** – Il docente ha il sospetto che stia avvenendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

In questo caso, l'informazione relativa al sospetto deve essere inoltrata al Referente e al team dei docenti "antibullismo" con l’obiettivo di allertare il Dirigente. La comunicazione dovrebbe avere una forma scritta e riportare tutti i dati e le informazioni in maniera dettagliata e oggettiva. Da qui, il Dirigente e i docenti coinvolti procedono alla valutazione del caso (valutare l’invio o meno della relazione agli organi giudiziari preposti) e agiscono tramite percorsi di sensibilizzazione.

**CASO B (EVIDENZA)** – Il docente ha evidenza certa che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

In questo caso, l'informazione relativa al sospetto deve essere inoltrata al Referente e al team dei docenti "antibullismo" con l'obiettivo di allertare il Dirigente. La comunicazione dovrebbe avere una forma scritta e riportare tutti i dati e le informazioni in maniera dettagliata e oggettiva.

Da qui, si procede alla valutazione approfondita e alla verifica di quanto segnalato, avviando (se appurato la rilevanza penale) la procedura giudiziaria con denuncia all'autorità giudiziaria per attivare un procedimento penale.

Qualora si rilevasse un fatto riconducibile alla fattispecie di reato, l'insegnante - nel ruolo di pubblico ufficiale – non deve procedere con indagini di accertamento ma ha sempre l'obbligo di segnalare l'evento all'autorità giudiziaria. (ex. l. 71/2017). Con autorità competente si intendono:

- Procure Ordinarie: nel caso in cui il minore/i sia la vittima/e e il presunto autore del reato sia maggiorenne,
- Procura Minorile: in caso il presunto autore del reato sia minorenni.

Vi è anche l'obbligatorietà della segnalazione delle situazioni di pregiudizio a carico dei minori: L. 216/1991: per le situazioni di grave rischio l'istituzione scolastica è tenuta alla segnalazione delle medesime. Per pregiudizio si intende una condizione di rischio o grave difficoltà che provocano un danno reale o potenziale alla salute, alla sopravvivenza, allo sviluppo o alla dignità del bambino, nell'ambito di una relazione di responsabilità, fiducia o potere.

La segnalazione come da procedura interna è il primo passo per aiutare un minore che vive una situazione di rischio o di grave difficoltà e va intesa come un momento di condivisione e solidarietà nei confronti del minore. La mancata segnalazione costituisce, infatti, omissione di atti d'ufficio (art.328 C.P.).

Può essere utile, valutando accuratamente ciascuna situazione, attivare colloqui individuali con tutti i minori coinvolti, siano essi vittime, testimoni e/o autori.

È importante considerare il possibile coinvolgimento dei genitori e di coloro incaricati della tutela dei minori coinvolti. L'intervento va indirizzato valutando l'eventuale impatto educativo e/o il contesto emotivo senza discriminare tra vittime, testimoni e/o autori.

Prevedere possibili incontri di mediazione tra i minori coinvolti vanno ponderati con la consapevolezza del loro stato emotivo, anche e in base agli elementi raccolti in merito del fatto/episodio avvenuto (elementi che si dovrebbero valutare di caso in caso). Importante è prevedere il coinvolgimento dei genitori sia della vittima che del bullo (ove possibile).

Anche i genitori devono e possono segnalare casi di sospetto o evidenza dei fenomeni, segnalarlo al Dirigente, o al docente coordinatore di classe o referente di istituto oppure direttamente al team antibullismo attraverso apposita procedura che definisce l'istituto (mail ad hoc, tramite gli uffici e postazioni specifiche, etc...).

Gli insegnanti e i genitori, come studenti e studentesse, si possono rivolgere alla Helpline del progetto Generazioni Connesse, al numero gratuito 19696, attraverso la chat disponibile sul [sito](#) o tramite chat WhatsApp per ricevere supporto e consulenza. Per tutti i dettagli, il riferimento è agli allegati con le procedure.

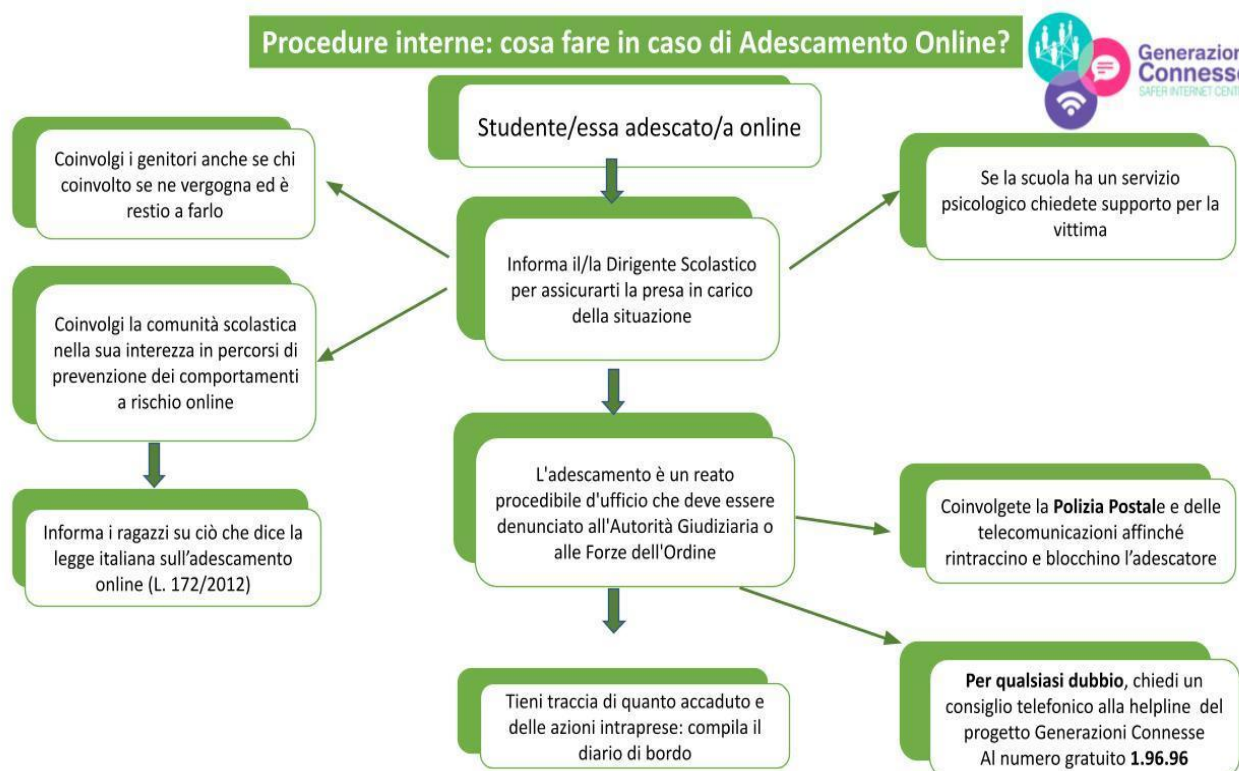
### Strumenti a disposizione di studenti/esse

Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola prevede alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola; sportello di ascolto con professionisti; docente referente per le segnalazioni.

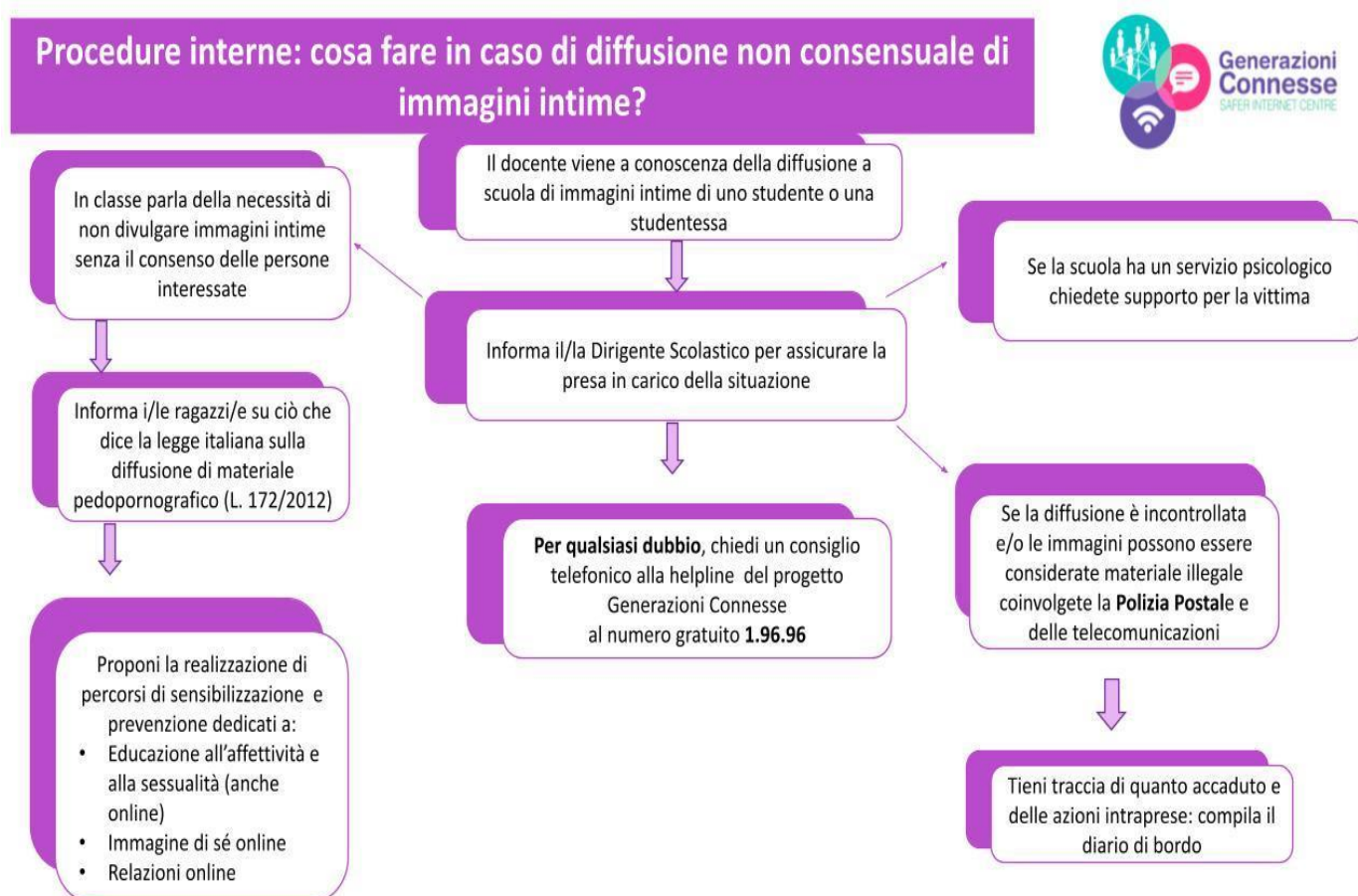
### GESTIONE DEI CASI:

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”.

### Cosa fare in caso di ADESCAMENTO

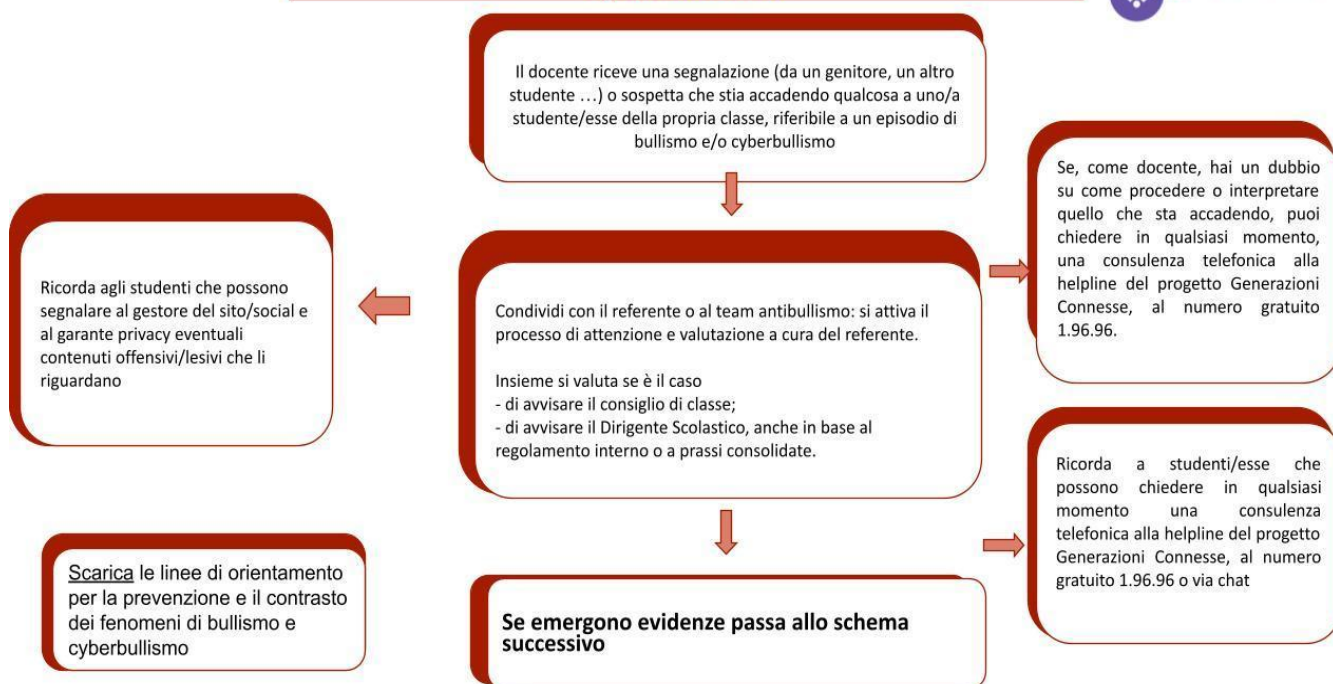


## Cosa fare in caso di SEXTING



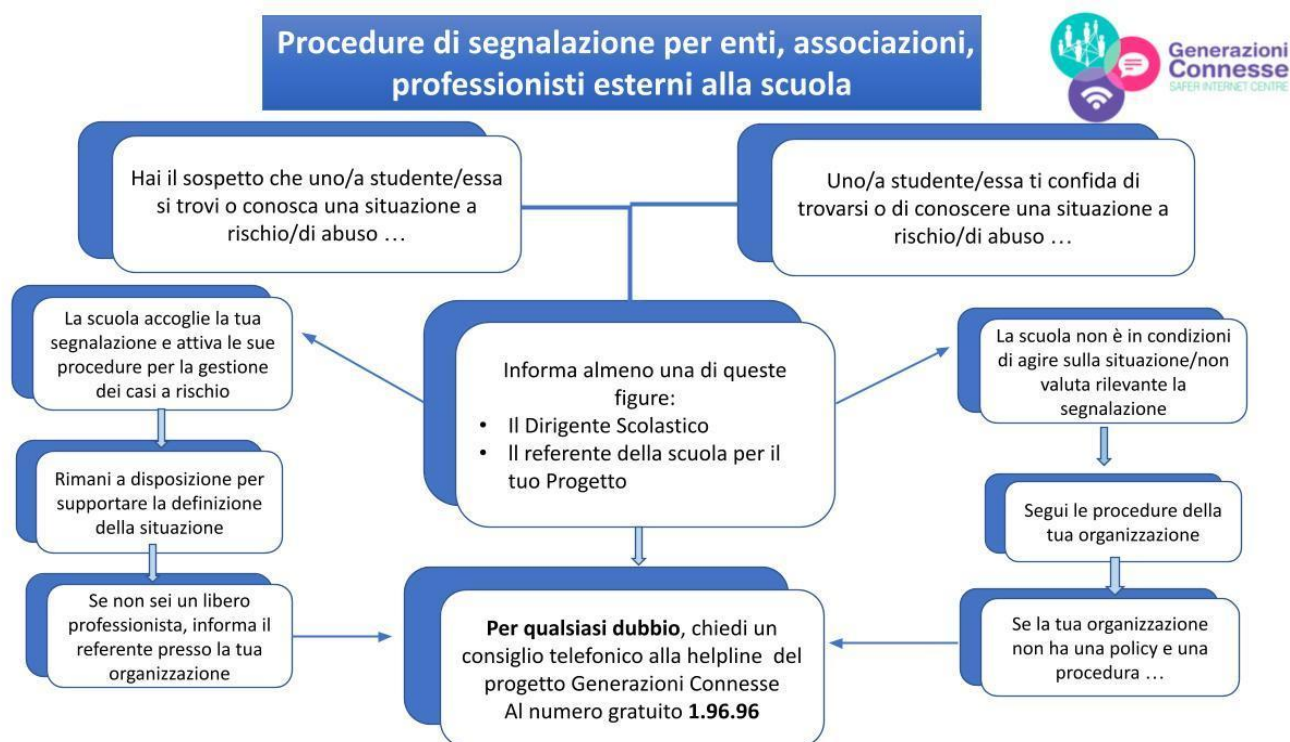
## Cosa fare in caso di CYBERBULLISMO

### Procedure interne: cosa fare in caso di sospetto di Cyberbullismo



### Procedure interne: cosa fare in caso di evidenza di Cyberbullismo





Si allega:

All.1 - Il diario di bordo

All.2 - Il modulo per segnalazione interna

All. 3 – Procedura di segnalazione interna – cyberbullismo

All.4 – Modulo per segnalazione Garante Privacy

All.5 – Tabella 1 – Protocollo di intervento nei casi di emergenza

All. 6 - Manifesto della Comunicazione Non Ostile

All.7- Decalogo: "Fake News- Basta Bufale"

All.8- Linee guida scuole per l'uso positivo delle tecnologie digitali e la prevenzione dei rischi nelle scuole

All. 9 - Kit didattico – Generazioni Connesse Teens /Generazioni Connesse Kids

All.10 – Guida per Genitori e Adulti di riferimento

Le premesse, gli allegati e tutti i documenti richiamati nella presente E – Safety Policy costituiscono parte integrante e sostanziale del documento

IL REFERENTE DEL BULLISMO

Prof. Francesco Giannotta

IL TEAM BULLISMO

Bandini Donato De Santis Maria Tridente Tiziana

LA DIRIGENTE SCOLASTICA

dott.ssa Giovanna Rotondo