ISTITUTO COMPRENSIVO
"Gian Giacomo Ciaccio Montalto"
Via Tunisi, 37 - 91100 TRAPANI – Tel 0923 20398 Telefax 0923 20106
CF: 80004160810 - C.M.: TPIC836004
e-mail tpic836004@istruzione.it – PEC tpic836004@pec.istruzione.it
www.icciacciomontalto.gov.it

Prot. n. 1278/D1/A1 Trapani, 09/02 /2018

E-SAFETY POLICY

(DISPOSITIVI E MISURE PER UNA POLITICA DI SICUREZZA)

A.S. 2017-2018

Documento approvato dal Collegio dei Docenti il 15/01/2018 e dal Consiglio d'Istituto il 09/02/2018

INDICE

1. INTRODUZIONE

1.1 SCOPO DELLA POLICY

Il documento vuole presentare in maniera chiara ed esaustiva le **linee guida dell'Istituto Comprensivo "G.G. Ciaccio Montalto"** in materia di:

• utilizzo consapevole delle TIC nella didattica e negli ambienti scolastici;

• prevenzione/gestione di situazioni problematiche relative all'uso delle tecnologie digitali.

La nostra scuola ha aderito al **progetto "Generazioni Connesse"**, promosso dal MIUR in collaborazione con la Comunità Europea, ed ha elaborato il presente documento in conformità con le Linee di orientamento per azioni di prevenzione e di contrasto al bullismo e cyberbullismo emanate dal Ministero dell'Istruzione, dell'Università e della Ricerca in collaborazione con il Safer Internet Center per l'Italia.
Il progetto "Generazioni connesse" sarà inserito nel nostro Piano Triennale dell'Offerta Formativa e le azioni preventivate nel Piano d'Azione della nostra scuola - prodotto nel mese di novembre 2017 - verranno portate avanti progressivamente nei prossimi anni.

Scopo del presente documento, che potrà essere revisionato annualmente, è quello di informare l'utenza per un uso corretto e responsabile delle apparecchiature informatiche collegate alla rete in dotazione alla Scuola, nel rispetto della normativa vigente.
Gli utenti, siano essi docenti o alunni, devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete. Di fatto esiste la possibilità che durante il lavoro online si possa entrare accidentalmente in contatto con materiale inadeguato e/o illegale, pertanto il nostro Istituto promuove l'adozione di strategie che limitino l'accesso a siti e/o applicazioni illeciti.
In questo contesto, gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di indicare regole di condotta chiare per un uso critico e consapevole di Internet anche a casa, per prevenire il verificarsi di situazioni potenzialmente pericolose.

Le **strategie previste dal nostro Istituto** per garantire la sicurezza in rete sono le seguenti:

- avvio di percorsi di formazione per un uso consapevole delle TIC rivolti agli insegnanti nel corso dell'anno scolastico;
- sviluppare moduli didattici:
  - per lo svolgimento di attività di ricerca, utilizzo critico delle fonti online e rielaborazione dei contenuti;
  - per la promozione del rispetto della diversità: rispetto delle differenze di genera, di orientamento e identità sessuale, di culture e provenienza, ecc.
- organizzare uno o più eventi/attività volti ad incrementare la partecipazione e lo scambio tra studenti, genitori e insegnanti;
- organizzare uno o più incontri dedicati alla prevenzione dei rischi associati all'utilizzo di Internet e delle tecnologie digitali, rivolti agli studenti, con il coinvolgimento di esperti;
- monitorare il tipo di utilizzo di Internet da parte degli studenti;
- controllo (una tantum e/o all'evenienza di episodi dubbi) del sistema informatico (cronologia, cookies, ecc.) da parte dei responsabili;
- installazione di firewall sull'accesso Internet;
- presenza di un docente o di un adulto responsabile durante l'utilizzo di Internet, delle piattaforme o di altre TIC;
- aggiornamento periodico del software antivirus e scansione delle macchine in caso di sospetta presenza di virus.

1.2 RUOLI E RESPONSABILITÀ

Il presente documento è condiviso da tutte le componenti educative che operano nella scuola ed in esso sono individuati ruoli e responsabilità correlate, così come di seguito indicati.

1) **Dirigente scolastico** dovrà:
− garantire la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri della comunità scolastica;
− garantire ai propri 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;
− garantire l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza on line;

2) **Animatore digitale,** come da PNSD, dovrà:
− 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.

3) **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.

4) **Docenti di tutte le discipline** dovranno:
− provvedere alla propria formazione/aggiornamento sull'utilizzo del digitale 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);
− 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;
− segnalare prontamente alle famiglie eventuali problematiche emerse in classe nell'utilizzo del digitale e stabilire comuni linee di intervento educativo per affrontarle;
− segnalare al Dirigente Scolastico e ai suoi collaboratori eventuali episodi di violazione delle norme di comportamento stabilite dalla scuola, avviando le procedure previste in caso di violazioni.

5) **Alunni** dovranno**:**
− ascoltare e seguire le indicazioni fornite dai docenti per un uso corretto e responsabile delle tecnologie digitali, attuando le regole di *e-safety* per evitare situazioni di rischio;
− chiedere l'intervento dell'insegnante, o dei genitori a casa, nello svolgimento dei compiti per mezzo del digitale, qualora insorgano difficoltà o dubbi nel suo utilizzo.

6) **Genitori** dovranno**:**
− contribuire, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete;
− incoraggiare l'impiego delle ICT da parte degli alunni nello svolgimento dei compiti a casa, controllando che tale impiego avvenga nel rispetto delle norme di sicurezza;
− agire in modo concorde con la Scuola per la prevenzione dei rischi e l'attuazione delle procedure

previste in caso di violazione delle regole stabilite;
− supportare le azioni intraprese dalla Scuola.

1.3 CONDIVISIONE E COMUNICAZIONE DELLA POLICY ALL'INTERA COMUNITÀ SCOLASTICA

Allo scopo di condividere regole comuni per l'utilizzo sicuro di Internet sia a casa che a scuola, si invitano tutti i genitori a prestare la massima attenzione ai principi e alle regole contenute nel presente documento. **Si richiede che ogni genitore e/o tutore si impegni a farle rispettare ai propri figli anche in ambito domestico, primariamente assistendo i minori nel momento dell'utilizzo della rete e poi ponendo in atto tutti i sistemi di sicurezza che aiutino a diminuire il rischio di imbattersi in materiale indesiderato.** La scuola promuove eventi e dibattiti informativi e formativi, in momenti diversi dell'anno, rivolti a tutto il personale, agli alunni e ai loro genitori, con il coinvolgimento di esperti, sui temi oggetto di questo documento. Tra le misure di prevenzione che la scuola mette in atto vi sono, inoltre, azioni finalizzate a promuovere una cultura dell'inclusione, del rispetto dell'altro e delle differenze così che l'utilizzo di Internet e dei cellulari, oltre che collocarci all'interno di un sistema di relazioni, ci renda consapevoli di gestire con un certo grado di trasparenza i rapporti che si sviluppano in tale ambiente, giungendo a riconoscere e gestire le proprie emozioni.

1.4 GESTIONE DELLE INFRAZIONI ALLA POLICY

Tutte le infrazioni alla presente Policy andranno tempestivamente segnalate al Dirigente Scolastico, che avrà cura di convocare le parti interessate onde valutare le possibili azioni da intraprendere. Il Dirigente Scolastico ha, altresì, la facoltà di revocare l'accessibilità temporanea o permanente ai laboratori e all'utilizzo di strumenti tecnologici (pc, tablet, notebook, smartphone, ecc.) a chi non si attiene alle regole stabilite.

1.5 MONITORAGGIO DELL'IMPLEMENTAZIONE DELLA POLICY E SUO AGGIORNAMENTO

Le regole relative all'accesso ad Internet vengono approvate dal Collegio dei Docenti e dal Consiglio di Istituto e pubblicate sul sito della scuola. I genitori/tutori sono invitati a rilasciare il consenso per l'accesso ad Internet e la dichiarazione liberatoria per la pubblicazione di elaborati, nomi, voci, immagini, materiale audiovisivo sul sito della scuola. (cfr. *Allegato 1* al Documento di E-Safety Policy). Gli alunni vengono informati del fatto che l'utilizzo di Internet è monitorato e vengono date loro istruzioni per un uso responsabile e sicuro (cfr. *Allegato 2* al Documento di E-Safety Policy). Tutto il personale scolastico è coinvolto nel monitoraggio dell'utilizzo di Internet, nello sviluppo delle linee guida e nell'applicazione delle istruzioni sull'uso corretto della rete (cfr. *Allegato 3* al Documento di E-Safety Policy).

1.6 INTEGRAZIONE DELLA POLICY CON I REGOLAMENTI ESISTENTI

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.

2. FORMAZIONE E CURRICOLO

2.1 CURRICOLO SULLE COMPETENZE DIGITALI PER GLI STUDENTI

Le Indicazioni Nazionale del 2012 in raccordo con il programma europeo Competenze chiave per un mondo in trasformazione prevedono che al termine del primo ciclo di istruzione lo studente possegga

buone competenze digitali e sappia usare con consapevolezza le tecnologie della comunicazione per ricercare e analizzare dati ed informazioni, per distinguere informazioni attendibili da quelle che necessitano di approfondimento, di controllo e di verifica e per interagire con soggetti diversi nel mondo. In questo senso le TIC (Tecnologie dell'Informazione e della Comunicazione) preparano gli studenti ad un'attiva e consapevole partecipazione ad un mondo in rapida evoluzione e nel quale è necessario acquisire abilità e competenze in grado di facilitare l'adattamento dell'individuo ai continui cambiamenti.
Si rende quindi necessario lo sviluppo e la diffusione di una mentalità tecnologica diffusa e precoce, intesa come alfabetizzazione al senso, all'utilizzabilità in contesti dati e per scopi definiti, da un lato ed acquisizione sempre più consapevole di strategie efficaci per il dominio di una macchina complessa che impiega e genera oggetti immateriali, dall'altro.
Gli alunni dovrebbero quindi imparare ad utilizzare le TIC per cercare, esplorare, scambiare e presentare informazioni in modo responsabile, creativo e con senso critico, essere in grado di avere un rapido accesso a idee ed esperienze provenienti da persone, comunità e culture diverse. Alla scuola spetta quindi anche il compito di trovare raccordi efficaci tra la crescente dimestichezza degli alunni con le Tecnologie dell'Informazione e della Comunicazione e l'azione didattica quotidiana. Le TIC possono infatti offrire significative occasioni per sviluppare le competenze di comunicazione, collaborazione e problem solving.

2.2 FORMAZIONE DEI DOCENTI SULL'UTILIZZO E L'INTEGRAZIONE DELLE TIC NELLA DIDATTICA

Il personale docente partecipa a corsi di formazione anche nell'ambito di piani nazionali, oltre che ad iniziative organizzate dall'istituzione o dalle scuole associate in rete e possiede generalmente una discreta base di competenze e, nel caso di alcune figure di sistema, anche di carattere specialistico.
È inoltre disponibile ad aggiornarsi per mantenere al passo la propria formazione, in rapporto al rinnovo della dotazione multimediale.
Il percorso complesso della formazione specifica dei docenti sull'utilizzo delle TIC nella didattica, non esauribile nell'arco di un anno scolastico, può, pertanto, prevedere momenti di autoaggiornamento, momenti di formazione personale o collettiva anche all'interno dell'istituto, con la condivisione delle conoscenze dei singoli ed il supporto dell'**Animatore digitale** e del **Team per l'innovazione**, la partecipazione alle iniziative promosse dall'Istituto e dalle scuole polo; può comprendere altresì la fruizione dei materiali messi a disposizione dall'Animatore stesso sulle bacheche virtuali appositamente create, corsi di aggiornamento online, ecc..

2.3 FORMAZIONE DEI DOCENTI SULL'UTILIZZO CONSAPEVOLE E SICURO DI INTERNET E DELLE TECNOLOGIE DIGITALI

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.
Sarà predisposta una bacheca online per la messa a disposizione e la condivisione di materiali per l'aggiornamento sull'utilizzo consapevole e sicuro di internet, collegata alla homepage del sito scolastico (www.icciacciomontalto.gov.it). Qui 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".

2.4 SENSIBILIZZAZIONE DELLE FAMIGLIE

L'Istituto attiverà iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC e della rete, promuovendo la conoscenza delle numerose situazioni di rischio online. A tal fine sono previsti incontri fra docenti e genitori per la diffusione del materiale informativo sulle tematiche trattate, messo a disposizione dai siti specializzati e dalle forze dell'ordine.
Saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi

fra i pari con l'uso di cellulari e smartphone o delle chat line o social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo.
Sul sito scolastico e sulla relativa bacheca virtuale relativa a "Generazioni connesse" saranno messi in condivisione materiali dedicati agli alunni e alle famiglie come guide in formato e video che possono fornire spunti di approfondimento e confronto. La scuola si impegna alla diffusione delle informazioni e delle procedure contenute nel documento Policy e-safety per portare a conoscenza delle famiglie il regolamento sull'utilizzo delle nuove tecnologie all'interno dell'Istituto e prevenire i rischi legati a un utilizzo non corretto di Internet.

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

3.1 ACCESSO AD INTERNET: FILTRI, ANTIVIRUS E SULLA NAVIGAZIONE

L'accesso a Internet è possibile in tutte le aule e nei laboratori d'informatica.
Le impostazioni sono definite e manutenute dal responsabile dei laboratori e dall'Animatore digitale ed è in carico a ciascun docente la segnalazione di malfunzionamenti e disservizi, al fine di richiedere, ove necessario, l'intervento di tecnici esterni.
I docenti hanno piena autonomia nel collegamento ai siti web nelle postazioni a loro riservate.
Relativamente agli alunni che accedono a Internet durante l'attività didattica sono consentiti la navigazione guidata da parte dell'insegnante e la stesura di documenti collaborativi purché sotto il controllo dell'insegnante e nel caso in cui tale attività faccia parte di un progetto di lavoro precedentemente autorizzato.

3.2 GESTIONE ACCESSI (PASSWORD, BACKUP, ECC...)

I computer portatili presenti nelle aule richiedono una password di accesso per l'accensione.
È possibile effettuare installazioni e aggiornamenti di software solo tramite la password di amministratore, fornita al personale di assistenza tecnica e all'Animatore Digitale.
Ogni docente è quindi tenuto ad un controllo della strumentazione in aula poiché l'uso del dispositivo è permesso agli alunni solo su autorizzazione dell'insegnante.
Ogni docente accede al registro elettronico attraverso una password personale che non può essere comunicata a terzi, né agli alunni.

3.3 SITO WEB DELLA SCUOLA

La Scuola è dotata di un sito istituzionale con estensione "gov.it" (www.icciacciomontalto.gov.it) sul quale diversi siti tematici rimandano al contenuto di interesse (pubblicità legale, circolari, ecc).
Pulsanti attivi permettono l'accesso a link di interesse tra cui il registro elettronico.
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.
Il personale che è in possesso delle credenziali per la gestione dei contenuti sul portale si assumerà la responsabilità editoriale di garantire che il contenuto inserito sia accurato e appropriato.

3.4 SOCIAL NETWORK

L'istituzione scolastica ha creato una pagina Facebook col proprio profilo (Istituto Comprensivo "G.G. Ciaccio Montalto" - Trapani) e ha autorizzato alcuni docenti a utilizzarla per nome e per conto della stessa sotto la supervisione del Dirigente Scolastico.

3.5 PROTEZIONE DEI DATI PERSONALI

L'Istituto Comprensivo "G.G. Ciaccio Montalto" rispetta la privacy dei propri utenti e si impegna a proteggere i dati personali che gli stessi conferiscono all'Istituto.
In generale, l'utente può navigare sul sito web della scuola senza fornire alcun tipo di informazione personale.

Il personale scolastico è "incaricato del trattamento" dei dati personali (degli alunni, dei genitori, ecc.), nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione).
L'istituto tratta i dati personali forniti dagli utenti in conformità alla normativa vigente.

4. STRUMENTAZIONE PERSONALE

4.1 PER GLI STUDENTI: GESTIONE DEGLI STRUMENTI PERSONALI

Ai sensi del Regolamento d'Istituto è tassativamente vietato l'utilizzo del telefono cellulare e di altri dispositivi elettronici durante tutte le attività scolastiche, sia per comunicare che per effettuare riprese video e/o sonore (C.M. del 15 marzo 2007).
Tuttavia ci si propone di aggiornare il suddetto Regolamento onde prevedere il BYOD (Bring Your Own Device) "porta il tuo dispositivo".
Riguardo agli alunni con disturbi specifici di apprendimento i genitori sono tenuti a concordare con i docenti le modalità di impiego di strumenti compensativi quali tablet e computer portatili.
Ai sensi della Direttiva Ministeriale n. 30 del 15 marzo 2007, con la condivisione della presente Policy, "le famiglie si assumono l'impegno di rispondere direttamente dell'operato dei propri figli nel caso in cui, ad esempio, gli stessi arrechino danni ad altre persone" a seguito di violazioni del presente regolamento.

4.2 PER I DOCENTI: GESTIONE DEGLI STRUMENTI PERSONALI

Ai sensi del Regolamento d'Istituto il divieto di utilizzare il cellulare è da intendersi rivolto a tutti i docenti della scuola salvo diverse autorizzazioni disposte dal Dirigente Scolastico per necessità motivate. Durante le ore delle lezioni, quindi, non è consentito l'utilizzo del cellulare, mentre è consentito l'uso di altri dispositivi elettronici personali solo a scopo didattico ed integrativo di quelli scolastici disponibili.

4.3 PER IL PERSONALE DELLA SCUOLA: GESTIONE DEGLI STRUMENTI PERSONALI

Ai sensi del Regolamento d'Istituto il divieto di utilizzare il cellulare è da intendersi rivolto a tutto il personale della scuola in servizio salvo diverse autorizzazioni disposte dal Dirigente Scolastico per necessità motivate.

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

5.1 PREVENZIONE

5.1.1 RISCHI

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, ma il loro ruolo diventa spesso inevitabilmente quello di confidenti degli alunni e delle loro esperienze. Proprio per questo, **gli insegnanti sono anche investiti del ruolo di una sorta di "torre di avvistamento", avamposto privilegiato delle problematiche e dei rischi che bambini e adolescenti possono trovarsi ad affrontare ogni giorno.**
La prima responsabilità degli insegnanti consiste, dunque, nell'imparare a riconoscere i rischi più comuni che i ragazzi possono correre sul web, per potere poi intervenire adeguatamente. Tra questi, un'attenzione specifica andrà prestata ai fenomeni di **bullismo/cyberbullismo** (una forma di prepotenza virtuale attuata attraverso l'uso di Internet e delle tecnologie digitali); **sexting** (pratica di inviare o postare messaggi di testo e immagini a sfondo sessuale, come foto di nudo o semi-nudo, via cellulare o tramite Internet) e **adescamento** o **grooming** (una tecnica di manipolazione psicologica, che gli adulti potenziali abusanti utilizzano online, per indurre bambini e adolescenti a superare le resistenze emotive e instaurare una relazione intima e sessualizzata).
I rischi che i ragazzi possono correre a scuola nell'utilizzo di dispositivi digitali possono derivare principalmente da un uso non corretto del telefono cellulare o di altri dispositivi come lo smartphone

o il tablet. Sebbene, infatti, l'uso del cellulare e dello smartphone non sia consentito dal Regolamento dell'Istituto, molti bambini della scuola primaria e quasi tutti i ragazzi della secondaria vengono a scuola con uno di questi dispositivi che dovrebbero comunque tenere spenti durante le lezioni.
Potrebbe accadere che in orario scolastico, alcuni studenti, eludendo la sorveglianza del personale della scuola, accendano e adoperino il cellulare o lo smartphone, non solo per comunicare con i propri genitori, ma anche per navigare su Internet, andando su siti non adatti e inviando materiali riservati (foto, video e altro). Così facendo, gli studenti possono incorrere anche a scuola nei rischi che abbiamo menzionato sopra, entrando in contatto e persino in confidenza con sconosciuti, fino a ricevere messaggi molesti e adescamenti.

5.1.2 AZIONI

L'obiettivo che l'insegnante deve proporsi dopo avere riconosciuto il pericolo è **agire** di conseguenza, con azioni di contrasto efficaci e mirate, rispetto ai rischi sopra elencati.
Tra le azioni utili a contrastare i rischi derivanti da un utilizzo improprio dei dispositivi digitali da parte degli studenti in orario scolastico, vi sono le seguenti:

- diffondere un'informazione capillare rivolta al personale scolastico, agli studenti e alle famiglie, sui rischi che i minori possono correre sul web, condividendo materiali messi a disposizione sul sito del progetto "Generazioni connesse";
- far rispettare il divieto di utilizzo di dispositivi digitali propri, quali cellulare e smartphone, agli
- studenti in orario scolastico;
- dotare i dispositivi della scuola di filtri che impediscano l'accesso a siti web non adatti ai minori (black list);
- bloccare l'accesso a un sito o a un insieme di pagine impedendone la consultazione;
- controllare periodicamente i siti visitati dagli alunni;
- utilizzare un software in grado di intercettare le richieste di collegamento e di respingere quelle non conformi alle regole stabilite dall'amministratore;
- affidare a un gruppo di docenti scelto le regole di filtraggio.

A tal proposito, la scuola proporrà incontri formativi atti a favorire momenti di riflessione e attività laboratoriali.

5.2 RILEVAZIONE

5.2.1 CHE COSA SEGNALARE

Può capitare che un alunno manifesti un'insofferenza nei confronti di un compagno o, al contrario, che un alunno si senta escluso o emarginato dai coetanei. In alcuni casi sono gli alunni stessi a rivolgersi ai docenti in cerca di aiuto, anche quando i fatti siano accaduti fuori dall'ambiente e dall'orario scolastico. La diffusione capillare dei social network tra i bambini e ancor più tra gli adolescenti, li espone sempre più spesso al rischio di inviare o condividere senza alcuna protezione materiali personali o riservati. Discutendo in classe dei rischi del web e confrontandosi sulle esperienze personali o dei propri coetanei, emergono spesso fatti che "allarmano" l'insegnante. Tuttavia, mentre l'insegnante ha la possibilità, anzi il dovere, di intervenire sui dispositivi digitali in uso a scuola, non può intervenire direttamente sui telefoni cellulari dei bambini senza un'esplicita autorizzazione delle famiglie.

<u>Tra i contenuti andranno opportunamente segnalati:</u>

- **contenuti afferenti la violazione della privacy**: foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, ecc.;
- **contenuti afferenti all'aggressività o alla violenza**: messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.;

- **contenuti riconducibili alla sfera sessuale**: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), ecc.

5.2.2 COME SEGNALARE: QUALI STRUMENTI E A CHI

Il personale della scuola, anche con l'ausilio del personale di assistenza tecnica e dell'Animatore digitale, dovrà provvedere a conservare le eventuali tracce di una navigazione non consentita su Internet o del passaggio di materiali inidonei sui pc della scuola; la data e l'ora consentiranno di condurre più approfondite indagini; nel caso di messaggi, si cercherà di risalire al mittente attraverso i dati del suo profilo. Sia nel caso di chat che di messaggi di posta elettronica, l'insegnante dovrà copiare e stampare i messaggi per fornire le eventuali prove dell'indagine sugli abusi commessi.
Tali prove saranno utili anche ad informare la famiglia dell'alunno vittima di abuso, il Dirigente Scolastico e, ove si configurino reati, la Polizia Postale.
In ogni caso, sarà opportuna una tempestiva informazione delle famiglie in merito all'accaduto, anche per consentire ulteriori indagini e, in assenza di prove oggettive, di raccogliere testimonianze sui fatti da riferire al Dirigente Scolastico ed, eventualmente, alla Polizia Postale.
Qualora siano coinvolti più alunni, in qualità di vittime o di responsabili della condotta scorretta, le famiglie degli alunni in questione saranno informate tempestivamente per un confronto.
In base all'entità dei fatti si provvederà:

1) a una comunicazione scritta tramite diario alle famiglie;
2) a una nota disciplinare sul registro di classe;
3) a una convocazione formale dei genitori degli alunni, tramite segreteria;
4) a una convocazione delle famiglie da parte del Dirigente Scolastico.

Per i reati più gravi gli operatori scolastici hanno l'obbligo di effettuare la denuncia all'autorità giudiziaria (o più semplicemente agli organi di polizia territorialmente competenti).
Inoltre ci si potrà avvalere dei due servizi messi a disposizione dal **Safer Internet Center** il **"Clicca e Segnala"** di **Telefono Azzurro e "STOP-IT" di Save the Children**. Una volta ricevuta la segnalazione, infatti, gli operatori procederanno a coinvolgere le autorità competenti in materia.

5.3 GESTIONE DEI CASI

5.3.1 DEFINIZIONE DELLE AZIONI DA INTRAPRENDERE A SECONDA DELLA SPECIFICA DEL CASO

a) Casi di cyberbullismo:

Si definiscono bullismo tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona (o a volte un piccolo gruppo). Si tratta, pertanto, di una serie di comportamenti portati avanti ripetutamente nel tempo. Si parla di cyberbullismo quando queste forme di prevaricazione reiterate nel tempo si estendono anche alla vita online. Tale specifica forma di bullismo ha caratteristiche peculiari:

1) è pervasivo: il bullo può raggiungere la sua vittima in qualsiasi momento e in qualunque luogo;
2) è un fenomeno persistente: il materiale messo online vi può rimanere per molto tempo;
3) spettatori e cyberbulli sono potenzialmente infiniti: le persone che possono assistere agli atti di cyberbullismo sono potenzialmente illimitate.

Occorre tenere presente che il cyberbullo non è mai del tutto consapevole della gravità dei suoi comportamenti se non viene aiutato ad esserne consapevole.
Qualora ci si trovi di fronte ad un caso di cyberbullismo si dovrà:

- informare i genitori degli alunni coinvolti;
- coinvolgere il referente di istituto dell'e-safety e gli operatori scolastici su quanto sta accadendo;
- coinvolgere la comunità scolastica in percorsi di prevenzione dei comportamenti a rischio online;
- tenere traccia di quanto successo e delle azioni intraprese, compilando un "diario di bordo" per

consentire ulteriori indagini se necessarie.

b) Casi di sexting:

Qualora ci si trovi di fronte a un caso di sexting (con cui si intende l'invio e/o la ricezione e/o la condivisione di testi, video o immagini sessualmente esplicite via cellulare o tramite internet) si dovrà:

- coinvolgere la classe e confrontarsi con esperti, facendo appello, per esempio, ad eventuali sportelli d'ascolto dell'istituto per capire come approfondire e affrontare il fenomeno;
- coinvolgere la comunità scolastica in percorsi di prevenzione dei comportamenti riconducibili al sexting;
- documentarsi opportunamente sulle norme giuridiche che regolano i comportamenti e le condotte sessuali in Italia;
- intraprendere con la classe attività mirate a riflettere sulla fiducia che ciascuno ripone negli altri e sul fenomeno del sexting, approfondendo casi e testimonianze.

c) Casi di adescamento online o *grooming*:

Le tecnologie digitali consentono ai giovani di ampliare la propria rete di amicizie in modo quasi smisurato: non di rado gli adolescenti "concedono" la loro amicizia non solo a persone che conoscono direttamente, ma anche ad "amici di amici". Questo li espone a rischi notevoli, come quello di dare accesso a sconosciuti al loro mondo online e quindi a informazioni personali.

L'adescamento online (*grooming*) consiste nel tentativo, da parte di un adulto, di avvicinare un bambino o un adolescente per scopi sessuali, conquistandone la fiducia attraverso l'utilizzo della rete Internet (tramite chat, blog, forum e social networks, per esempio). In un primo tempo, l'adulto, spesso mentendo sulla propria identità e sulla propria età, mostra particolare interesse nei confronti del bambino o dell'adolescente, cercando di conquistarne la fiducia. Solo in un secondo tempo, cerca di entrare sempre più nell'intimità fino ad introdurre argomenti intimi e attinenti alla sfera sessuale.

È giusto che anche gli insegnanti aiutino i propri alunni a tutelarsi, scegliendo con cura chi frequentare online, per evitare che una condotta imprudente possa comportare ripercussioni non banali nella loro vita reale. Una volta riconosciuti alcuni segni che possono rinviare a una situazione di adescamento online, quali un improvviso calo nel rendimento scolastico; un aumento del tempo trascorso dall'alunno online congiunto ad una particolare riservatezza al riguardo; allusioni da parte dell'alunno alla frequentazione di una persona più grande, o a regali ricevuti, ecc., è bene:

- approfondire la situazione coinvolgendo la classe e l'intera comunità scolastica;
- avviare dei percorsi di riflessione in classe sul concetto di fiducia;
- farsi affiancare da esperti, ricorrendo anche ad eventuali sportelli d'ascolto per offrire ai minori, qualora lo desiderino, il supporto necessario.

ALLEGATI:

Allegato 1 - Documento di E-Safety Policy: Consenso dei genitori/tutori per l'accesso ad Internet e dichiarazione liberatoria per la pubblicazione di elaborati, nomi, voci, immagini, materiale audiovisivo sul sito della scuola.

Allegato 2 - Documento di E-Safety Policy: Assunzione di responsabilità da parte degli Studenti per l'uso consapevole di Internet.

Allegato 3 - Documento di E-Safety Policy: Assunzione di responsabilità da parte di Docenti e altro Personale della Scuola.

CONSENSO DEI GENITORI/TUTORI PER L'ACCESSO AD INTERNET E DICHIARAZIONE LIBERATORIA PER LA PUBBLICAZIONE DI ELABORATI, NOMI, VOCI, IMMAGINI, MATERIALE AUDIOVISIVO

Al Dirigente dell'I.C. Ciaccio Montalto
di Trapani

I sottoscritti ..... e .....,

genitori/tutori dell'alunno/a ..... iscritto/a alla classe ..... sez. .....

della scuola dell'infanzia/primaria/secondaria di 1° grado .....

Dichiarano

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

Pertanto, i sottoscritti

- **acconsentono/non acconsentono** (*barrare la voce che non interessa*) che il/la proprio/a figlio/a utilizzi a scuola l'accesso Internet;
- **autorizzano/non autorizzano** *(barrare la voce che non interessa)* l'Istituto Comprensivo "G.G. Ciaccio Montalto" a realizzare e ad utilizzare, a scopo didattico e/o di documentazione e/o di informazione e senza fini di lucro, fotografie, video o altri materiali audiovisivi contenenti l'immagine, il nome, la voce, gli elaborati (scritti, disegni, ...) del/la proprio/a figlio/a anche, se del caso, mediante riduzioni e/o adattamenti;
- **dichiarano** di essere informati che detto materiale potrà essere utilizzato per documentare e divulgare le attività della scuola tramite il sito Internet di Istituto, pubblicazioni, cd-rom, mostre, seminari, convegni e altre iniziative promosse dalla scuola anche in collaborazione con altri soggetti;
- **dichiarano** di non aver nulla a pretendere in ragione di quanto sopra indicato e di rinunciare irrevocabilmente ad ogni diritto, azione o pretesa derivante da quanto sopra autorizzato.

Allegato:
Fotocopie dei documenti di identità

Firma Firma

....

Trapani, ...

ASSUNZIONE DI RESPONSABILITÀ DA PARTE DEGLI STUDENTI PER L'USO CONSAPEVOLE DI INTERNET

Al Dirigente dell'I.C. Ciaccio Montalto
di Trapani

Il/La sottoscritto/a ....., alunno/a della Classe ....., Sez. ..... della Scuola Secondaria di 1° grado dell'I.C. "G.G. Ciaccio Montalto" di Trapani

Dichiara

- di aver letto e compreso il **Documento di E-Safety Policy**;
- di essere consapevole che, a seguito di violazione volontaria delle regole in esso contenute, la Scuola avrà il diritto di sospendere l'accesso ad Internet e di adottare le sanzioni disciplinari previste.

Pertanto, il/la sottoscritto/a

si impegna a:

utilizzare le Tecnologie dell'Informazione e della Comunicazione (TIC) e la navigazione in Internet in modo responsabile, secondo le regole previste dal **Documento di E-Safety Policy**.

Firma

.....

Trapani, ...

ASSUNZIONE DI RESPONSABILITÀ DA PARTE DI DOCENTI E ALTRO PERSONALE DELLA SCUOLA

Al Dirigente dell'I.C. Ciaccio Montalto
di Trapani

Il/La sottoscritto/a ....., dipendente dell'I.C. "G.G. Ciaccio Montalto" di Trapani, in qualità di .....

Dichiara:

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

Pertanto, il/la sottoscritto/a

si impegna a:

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

Firma

.....

Trapani, ...