



Cambridge English

Exam Preparation Centre



Ministero dell'Istruzione
dell'Università e della Ricerca



ISTITUTO COMPRENSIVO "G. CALÒ"

V.le M. UNGHERIA, 86 - 74013 GINOSA (TA)

tel. +390998245663 - E-mail: TAIC82600L@istruzione.it - PEC: TAIC82600L@pec.istruzione.it

Sito web: www.scuolacalo.edu.it - C.F. 90122060735

E- Safety Policy

Indice

- 1. Introduzione**
 - 1.1 Scopo della Policy.
 - 1.2 Ruoli e Responsabilità.
 - 1.3 Condivisione e comunicazione della Policy all'intera comunità scolastica.
 - 1.4 Gestione delle infrazioni alla Policy.
 - 1.5 Monitoraggio dell'implementazione della Policy e suo aggiornamento.
 - 1.6 Integrazione della Policy con Regolamenti esistenti.
- 2. Formazione e Curricolo**
 - 2.1 Curricolo sulle competenze digitali per gli studenti.
 - 2.2 Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica.
 - 2.3 Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
 - 2.4 Sensibilizzazione delle famiglie.
- 3. Gestione dell'infrastruttura e della strumentazione ICT della scuola.**
 - 3.1 Accesso ad internet: filtri, antivirus e sulla navigazione.
 - 3.2 Gestione accessi
 - 3.3 Sito web della scuola
 - 3.4 Social network
 - 3.5 Protezione dei dati personali
- 4. Strumentazione personale**
 - 4.1 Per gli studenti: gestione degli strumenti personali - cellulari, tablet ecc..
 - 4.2 Per i docenti: gestione degli strumenti personali - cellulari, tablet ecc..
 - 4.3 Per il personale della scuola: gestione degli strumenti personali - cellulari, tablet ecc.
- 5. Prevenzione, rilevazione e gestione dei casi**
 - 5.1 Prevenzione
 - 5.1.1 Rischi
 - 5.1.2 Azioni
 - 5.2 Rilevazione
 - 5.2.1 Che cosa segnalare
 - 5.2.2 Come segnalare: quali strumenti e a chi.
 - 5.3 Gestione dei casi
 - Definizione delle azioni da intraprendere a seconda della specifica del caso.

1. Introduzione

L'Istituto Comprensivo "G. Calò" ha ritenuto opportuno dotarsi di una policy di e-safety per essere pronto a cogliere i cambiamenti in atto nell'attuale società della conoscenza in cui opera, in particolare per quanto riguarda la formazione dei cittadini del futuro, destinati a vivere in un ambiente in cui tutto viene gestito attraverso l'utilizzo delle Tecnologie dell'Informazione e della Comunicazione (TIC). Tali tecnologie diventano abilitanti, quotidiane, ordinarie, al servizio dell'attività scolastica e di tutti i suoi ambienti, coinvolgendo sia le attività orientate alla formazione e all'apprendimento sia l'amministrazione, con ricadute estese al territorio. Con questo documento si vuole regolamentare l'uso di Internet per rendere responsabili tutti gli utenti dell'Istituto in modo tale da garantire la privacy all'interno dei plessi e degli uffici di segreteria. Le indicazioni nazionali pongono l'accento sulle competenze digitali degli studenti, ai quali è richiesto di sapersi orientare nelle molteplici possibilità offerte dal Web, analizzando criticamente i materiali disponibili, scambiando informazioni ed esperienze in modo consapevole e responsabile. Occorre in tal senso informare e formare le componenti scolastiche, in particolare gli alunni, in merito a eventuali rischi e fornire misure atte a prevenirli, permettendo di beneficiare in sicurezza delle opportunità offerte da Internet e dalle TIC.

Al termine del documento è inserito un glossario per una migliore comprensione. La policy di e-safety verrà revisionata e aggiornata periodicamente in base a eventuali variazioni delle norme, delle dotazioni tecnologiche e dei protocolli dell'Istituto.

1.1 Scopo della Policy

Le tecnologie digitali sono sempre più presenti nella vita quotidiana di tutti, così come negli ambienti scolastici, e bambini e adolescenti entrano in contatto con esse in età sempre più precoce. La presenza di tali tecnologie offre senza dubbio nuove opportunità a livello didattico, alle quali si accompagna la necessità di operare riflessioni e interventi volti ad un utilizzo che possa definirsi sicuro, consapevole e positivo in primo luogo da parte dei ragazzi, ormai "nativi digitali", che delle tecnologie fanno un uso immediato e spesso poco consapevole proprio in virtù della grande diffusione delle tecnologie e della apparente semplicità che contraddistingue il loro utilizzo.

È pertanto necessario, da parte delle Istituzioni Scolastiche, avviare una politica di sicurezza della navigazione on line volta ad un controllo dell'uso delle strumentazioni digitali e alla diffusione dell'adozione di buone pratiche di navigazione su Internet. Se bambini e giovanissimi mostrano un'innata predisposizione all'uso delle tecnologie, tuttavia, assai frequentemente a questa abilità non corrisponde una adeguata e corretta capacità interpretativa della mole di informazioni alla quale essi sono di continuo sottoposti, in primo luogo attraverso i social network, i quali, se utilizzati in modo superficiale e inappropriato, possono trasformarsi in veicoli di cyber-bullismo.

Dall'esistenza di questo bisogno di promozione di un uso sicuro e positivo delle tecnologie scaturisce il presente documento, prodotto dalla Scuola nell'ambito dell'adesione - a partire dal presente anno scolastico - al progetto "Generazioni connesse", promosso dal Miur per offrire alle Istituzioni Scolastiche interessate un supporto effettivo nella definizione di misure di prevenzione, rilevazione e gestione delle problematiche derivanti da un uso non consapevole delle tecnologie digitali tra gli studenti, anche attraverso la formazione degli insegnanti e la sensibilizzazione dei genitori. In sintesi, il documento intende semplicemente costituire un primo step in questa direzione e fornire alcune linee guida rispetto alle azioni dell'Istituto in ordine a: utilizzo consapevole delle TIC in ambiente scolastico e nella didattica prevenzione e gestione di situazioni problematiche connesse all'uso delle tecnologie digitali

Ruoli e Responsabilità

Nell'ambito di questa policy sono individuati i seguenti ruoli e le principali responsabilità correlate:

Dirigente scolastico:

- ✓ 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) che consenta loro di possedere le 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.

Animatore digitale, come da PNSD:

- ✓ *Formazione interna* - 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, come ad esempio quelle organizzate attraverso gli snodi formativi;
- ✓ *Coinvolgimento della comunità scolastica* - favorire la partecipazione e stimolare il protagonismo degli studenti nell'organizzazione di workshop e altre attività, anche strutturate, sui temi del PNSD, anche attraverso momenti formativi aperti alle famiglie e ad altri attori del territorio, per la realizzazione di una cultura digitale condivisa;
- ✓ *Creazione di soluzioni innovative* - 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.

Direttore dei Servizi Generali e Amministrativi:

- ✓ 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;
- ✓ 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.

Docenti:

- ✓ provvedere personalmente alla propria formazione/aggiornamento sull'utilizzo del digitale con particolare riferimento alla dimensione etica (tutela della privacy, rispetto dei diritti intellettuali dei materiali reperiti in Internet e dell'immagine degli altri: lotta al cyberbullismo);
- ✓ 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.

Allievi:

- ✓ 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 e/o dei genitori nello svolgimento dei compiti a casa per mezzo del digitale, qualora insorgano difficoltà o dubbi nel suo utilizzo.

Genitori:

- ✓ 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.

1.2 Condivisione e comunicazione della Policy all'intera comunità scolastica

Per evitare che l'adozione di questa policy rappresenti un mero atto formale, l'Istituto

si impegna a prendere spunto da essa come base di partenza per una serie di azioni e iniziative.

Per il personale scolastico:

- Le norme adottate dalla scuola in materia di sicurezza nell'utilizzo del digitale saranno discusse negli organi collegiali (collegio docenti, riunioni di dipartimento, consigli di classe) e rese note all'intera comunità scolastica tramite pubblicazione del presente documento sul sito web della scuola.
- Il personale della scuola riceverà un'adeguata informazione/formazione sull'uso sicuro e responsabile di internet, attraverso materiali resi disponibili anche sul sito web della scuola.

Per gli studenti:

- All'inizio dell'anno, in occasione della illustrazione del regolamento d'istituto agli alunni da parte dei docenti, verrà presentata questa policy, insieme ai regolamenti correlati.
- Nel corso dell'anno saranno dedicate da ciascun docente alcune lezioni alle buone pratiche per un utilizzo sicuro del digitale, con specifico riferimento ai rischi della rete e alla lotta al cyberbullismo.

Per i genitori:

- l'organizzazione di incontri di sensibilizzazione sul tema della sicurezza informatica e di informazione circa i comportamenti da monitorare o da evitare.

1.3 Gestione delle infrazioni alla Policy

In relazione a quanto specificato in questa policy le infrazioni saranno gestite in modo graduale rispetto alla gravità dell'infrazione e, nel caso degli alunni, anche rispetto alla loro età.

Infrazioni degli alunni

È bene che i docenti introducano, preventivamente, attività laboratoriali miranti a sviluppare nei loro alunni una sempre maggiore consapevolezza dei rischi legati a un uso imprudente e improprio del web e che forniscano loro, ogni qualvolta avvenga un'infrazione alle regole stabilite, gli strumenti per affrontare le conseguenze dei loro errori.

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 (assegnazione di attività aggiuntive da svolgere a casa su temi di Cittadinanza e Costituzione/ Ed. Civica/ Educazione alla Cittadinanza Digitale, divieto temporaneo di prendere parte alla ricreazione e simili);
- ✓ nota informativa sul diario ai genitori;
- ✓ convocazione dei genitori per un colloquio con l'insegnante;

- ✓ convocazione dei genitori per un colloquio con il Dirigente scolastico.

Infrazioni del personale scolastico

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

Nel primo caso la gravità si valuta sull'esposizione al rischio procurata agli alunni, nel secondo caso sul danno per la non tempestiva attivazione delle azioni qui indicate.

La gestione delle infrazioni in quest'ambito ricade nella disciplina contrattuale.

Infrazioni dei genitori

Compito precipuo dei genitori è supportare gli insegnanti e il personale scolastico nel riconoscimento e nella costruzione di azioni di contrasto efficaci ai principali rischi rappresentati dalla navigazione in internet di utenti molto giovani e spesso poco accorti. Nel caso di infrazione si prevedono interventi, rapportati alla sua gravità, che vanno dalla semplice comunicazione del problema alla convocazione da parte dell'insegnante di classe o del Dirigente Scolastico.

1.4 Monitoraggio dell'implementazione della Policy e suo aggiornamento

Il monitoraggio dell'implementazione della Policy avverrà:

- ✓ alla fine di ogni anno scolastico, contestualmente al Rapporto di Autovalutazione e sulla base dei casi problematici riscontrati e della loro gestione;
- ✓ all'inizio di ogni anno scolastico, contestualmente alla revisione del PTOF, a cura del Dirigente scolastico, dell'Animatore digitale e dei collaboratori del Dirigente, a seguito di verifica atta a constatare l'insorgenza di nuove necessità e la revisione di tecnologie esistenti.

1.5 Integrazione della Policy con 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, incluso il piano per l'attuazione del PNSD;
- ✓ Regolamento interno d'istituto;

La policy richiede l'integrazione con l'inserimento delle seguenti norme:

UTILIZZO DEL LABORATORIO DI INFORMATICA, DELLE POSTAZIONI DI LAVORO E DELL'UTILIZZO DI INTERNET

Disposizioni sull'uso del laboratorio

1. Le apparecchiature presenti nella scuola sono un patrimonio comune, quindi, vanno utilizzate con il massimo rispetto.
2. I laboratori informatici e le postazioni informatiche dell'istituto possono essere utilizzati esclusivamente per attività di insegnamento, funzionali all'insegnamento e di formazione del personale docente e non docente.
3. Quando un insegnante, da solo o in classe, usufruisce del laboratorio deve obbligatoriamente registrare il proprio nome e l'eventuale classe nell'apposito registro delle presenze di laboratorio, indicando l'orario di ingresso, quello di uscita e motivazione dell'uso delle postazioni informatiche. Questo allo scopo di poter risalire alle cause di eventuali inconvenienti o danneggiamenti e per comprovare l'effettivo utilizzo dell'aula.
4. L'ingresso degli allievi nei laboratori è consentito solo in presenza dell'insegnante.
5. Il docente accompagnatore è responsabile del corretto uso didattico di hardware e software.
6. Nei laboratori è vietato utilizzare CD personali o dischetti se non dopo opportuno controllo con sistema di antivirus aggiornato.
7. È vietato cancellare o alterare files-dati presenti sull'hard disk.
8. Il laboratorio non deve mai essere lasciato aperto o incustodito quando nessuno lo utilizza. All'uscita dal laboratorio sarà cura di chi lo ha utilizzato lasciare il mobilio in ordine, le macchine spente correttamente (chiudi sessione...).
9. In caso di malfunzionamento o guasto dei computer bisogna darne tempestiva segnalazione al responsabile del laboratorio.
10. In caso di malfunzionamento non risolvibile dal responsabile di laboratorio si contatterà personalmente o attraverso il Responsabile di laboratorio, il DSGA.
11. Per motivi di manutenzione straordinaria, in caso di guasti o di virus, i PC possono essere formattati senza preavviso. Si consiglia pertanto di salvare i dati importanti su Cd o pen drive periodicamente. In caso di formattazione ordinaria ci sarà un preavviso.

Disposizioni sull'uso dei software

1. I software installati sono ad esclusivo uso didattico.
2. In base alle leggi che regolano la distribuzione delle licenze, i prodotti software presenti in laboratorio non sono disponibili per il prestito individuale. Nei casi in cui lo fossero in base a precise norme contrattuali i docenti interessati, dopo aver concordato il prestito con il Responsabile di laboratorio, devono compilare l'apposito registro di consegna software custodito in laboratorio.

3. È fatto divieto di usare software non conforme alle leggi sul copyright. È cura dell'insegnante-utente di verificarne la conformità. Gli insegnanti possono installare nuovo software sui PC del laboratorio previa autorizzazione scritta del Responsabile di laboratorio. Si raccomanda, quindi, di verificare che il software installato rispetti le leggi sul copyright.

4. È responsabilità degli insegnanti che chiedono al Responsabile di laboratorio di effettuare copie di cd/dvd per uso didattico, di assicurarsi che la copia non infranga le leggi sul copyright in vigore.

Accesso a internet

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

2. Internet non può essere usato per scopi vietati dalla legislazione vigente;

3. L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet;

4. È vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare software non autorizzati da internet, scaricare e installare software senza licenza.

Norme finali

Il Responsabile di laboratorio che verifichi un uso del laboratorio contrario a disposizioni di legge o del regolamento interno deve darne comunicazione per iscritto al Dirigente Scolastico.

2. Formazione e Curricolo

2.1 Curricolo sulle competenze digitali per gli studenti

Le TIC e Internet sono un elemento essenziale nella vita del XXI secolo. La scuola ha il dovere di fornire alla componente studentesca l'accesso a questi strumenti come parte della loro esperienza di apprendimento e di far maturare in loro le competenze per una proficua cittadinanza digitale.

L'uso delle TIC, pertanto, è stato inserito nel curricolo sia a livello disciplinare sia a livello interdisciplinare.

In particolare il curricolo è stato strutturato per prevedere al termine della scuola primaria e al termine del primo ciclo di istruzione le competenze digitali in base ai seguenti profili:

- primaria: usa le tecnologie in contesti comunicativi concreti per ricercare dati e informazioni e per interagire con soggetti diversi.

- secondaria di primo grado: usa 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.

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

Il corpo docente ha partecipato 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 buona base di competenze e, nel caso delle 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.

All'interno dell'istituto, infine, con la condivisione delle conoscenze dei singoli e il supporto dell'Animatore digitale, la formazione avviene anche attraverso la fruizione dei materiali messi a disposizione dall'Animatore stesso sulle bacheche virtuali e attraverso corsi di aggiornamento online.

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.scuolacalo.edu.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

Il nostro istituto ha organizzato già negli anni passati incontri aperti alle famiglie e agli studenti con enti esterni, come la Polizia Postale, per sensibilizzare docenti, alunni e genitori sui temi della sicurezza online. Anche nei prossimi anni si continuerà ad utilizzare questo approccio per la sensibilizzazione delle famiglie, con incontri che offriranno occasione di confronto e discussione sui rischi rappresentati dall'uso di cellulari, smartphone e chat line senza un'adeguata formazione in merito ai rischi derivanti da un uso inappropriato di tali dispositivi. Sul sito scolastico saranno resi accessibili i materiali dedicati alle famiglie e ai ragazzi nella [bacheca virtuale del sito](#)

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 all'interno dell'istituto e favorire un'attiva collaborazione tra la scuola e le famiglie sui temi della prevenzione dei rischi connessi a un uso inappropriato del digitale.

3. Gestione dell'infrastruttura e della strumentazione ICT della Scuola

3.1 Accesso ad internet: filtri, antivirus e sulla navigazione

L'accesso a internet è possibile nella scuola primaria e nella scuola secondaria in tutte le aule, dotate di Lavagna Interattiva Multimediale con relativo computer portatile, custodito in un cassetto chiuso a chiave, e nei laboratori d'informatica. Le impostazioni sono definite e mantenute dal responsabile tecnico dei laboratori ed è in carico a ciascun docente la segnalazione di malfunzionamenti e disservizi.

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 portatile presenti nelle aule non richiedono una password di accesso per l'accensione. 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.

Nei computer presenti nei laboratori sono previsti tre profili di accesso con password relative:

- ✓ amministratore;
- ✓ docente;
- ✓ alunno.

È possibile effettuare installazioni e aggiornamenti di software solo tramite la password di amministratore, fornita al personale di assistenza tecnica e/o all'Animatore Digitale.

3.3 Sito web della scuola

Il sito dell'Istituto Comprensivo è www.scuolacalo.edu.it

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 usufruisce della piattaforma di “social learning” Fidenia in cui gli insegnanti possono dialogare con i propri alunni e con i colleghi, ognuno col proprio profilo. Con Fidenia ogni docente può creare classi virtuali, inviare compiti e questionari auto-valutanti, assegnare voti, condividere idee e materiale didattico in maniera rapida ed efficace.

3.5 Protezione dei dati personali

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). Tutto il personale incaricato riceve poi istruzioni particolareggiate applicabili al trattamento di dati personali ai fini della protezione e sicurezza degli stessi.

In caso di attività di ampliamento dell'offerta formativa, organizzate in collaborazione con Enti esterni, viene richiesto preventivamente ai genitori il consenso informato alle riprese audio/ video e al loro eventuale utilizzo per scopi didattici, informativi e divulgativi anche tramite pubblicazione su siti web.

L'accesso ai dati riportati nel registro elettronico (ritardi, assenze, note e valutazioni) è riservato ai genitori tramite la consegna di una password di accesso strettamente personale.

4. Strumentazione personale

4.1 Per gli studenti: gestione degli strumenti personali – cellulari, tablet ecc.

Non è consentito agli studenti alcun uso di strumenti elettronici personali né quello del cellulare.

Nella scuola primaria si chiede alle famiglie di non lasciare tali dispositivi ad alunne e alunni; nella scuola secondaria di primo grado all'ingresso in aula, dopo l'appello, la componente studentesca deposita eventuali telefoni e altri dispositivi sulla cattedra dove rimangono in custodia al corpo docente che si alterna durante le lezioni.

Nel caso in cui gli studenti debbano comunicare con la famiglia durante l'orario scolastico, possono usare gratuitamente la linea fissa della scuola rivolgendosi a un operatore; allo stesso modo le famiglie devono chiamare il centralino della scuola se hanno assoluta necessità di parlare con i propri figli. Tali comunicazioni saranno ridotte a casi di inderogabile necessità e urgenza.

Gli alunni con disturbi specifici di apprendimento concorderanno le modalità di impiego di strumenti compensativi quali tablet e computer portatili e le modalità di custodia.

4.2 Per i docenti: gestione degli strumenti personali– cellulari, tablet ecc.

Durante le ore delle lezioni 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.

Durante il restante orario di servizio è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente mentre è permesso l'uso di altri dispositivi elettronici personali per attività funzionali all'insegnamento, ad integrazione di quelli scolastici disponibili.

4.3 Per il personale della scuola: gestione degli strumenti personali – cellulari, tablet ecc.

Durante l'orario di servizio al restante personale scolastico è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente.

4.4 Prevenzione, rilevazione e gestione dei casi

4.5 Prevenzione

4.5.1 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, sexting e adescamento o grooming**.

4.5.2 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 alunni 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.

4.6 Rilevazione

4.6.1 *Che cosa segnalare*

Si considerano da segnalare tutte quelle situazioni caratterizzate da *volontarie e ripetute aggressioni* mirate a insultare, minacciare, diffamare e/o ferire una persona (o un piccolo gruppo) tramite un utilizzo irresponsabile dei social network.

In particolare si segnaleranno:

- ✓ 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 afferenti alla sessualità: 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.

Tutte le segnalazioni riportate dai docenti verranno registrate su apposita scheda (in coda al documento).

4.6.2 *Come segnalare: quali strumenti e a chi.*

Gli insegnanti, anche con l'ausilio del tecnico e/o del Team Digitale, possono provvedere a conservare le prove della condotta incauta, scorretta o dell'abuso rilevate sui pc della scuola: soprattutto la data e l'ora, il contenuto dei messaggi e, se possibile, l'ID del mittente (es. username, mail, numero di telefono cellulare) o l'indirizzo web del profilo ed il suo contenuto. Per il telefono cellulare ci si può assicurare che l'alunno vittima salvi nel suo telefono ogni messaggio, voce/testo/immagine, conservando così il numero del mittente.

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

Qualora non si disponga di prove, ma solo delle testimonianze dell'alunno, quantunque riferite a fatti accaduti al di fuori del contesto scolastico, le notizie raccolte sono comunque comunicate ai genitori e per fatti rilevanti anche al Dirigente scolastico.

In particolare la segnalazione viene fatta a entrambe le famiglie, se oltre alla vittima

anche l'autore della condotta negativa è un altro alunno.

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.

In base all'urgenza le comunicazioni formali possono essere precedute da quelle informali, effettuate per le vie brevi.

Per i reati più gravi (es. pedopornografia) 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.

4.7 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" e dalla Piattaforma Elisa.

Ginosa, 10 febbraio 2020

Il Dirigente Scolastico
Prof.ssa Marianna Galli
(f.to digitalmente)