

Istituto Comprensivo Ilaria Alpi - Torino

sede amministrativa - s.s.p.g. B. Croce corso Novara 26

Sc. Infanzia - G. Perempruner Via Vittorio Bersezio 11

Sc. Primaria - G. Perotti - Via Mercadante, 68/8

Sc. Primaria S. D'Acquisto - Via Tollegno, 83

Sc. Primaria G. Deledda - Via Bologna, 77

Cod. M.I.U.R.: TOIC8BD00X

Centralino: Tel. 011/2481916 Segreteria: Tel. 011/2481916

TOIC8BD00X@istruzione.it TOIC8BD00X@pec.istruzione.it



E-Safety Policy

Anno Scolastico 2017-2018

Prot. nr

Sommario

1. Introduzione

- 1.1 Scopo della Policy.
- 1.2 Ruoli e Responsabilità della Comunità Scolastica.
- 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 (password, backup, ecc.).
- 3.3. E-mail.
- 3.4 Blog e sito web della scuola.
- 3.5 Social network.
- 3.6 Protezione dei dati personali.

4. Strumentazione personale

- 4.1 Gestione degli strumenti personali .

5. Prevenzione, rilevazione e gestione dei casi

- Prevenzione.
- Azioni.

1. Introduzione

Le nuove Tecnologie Informatiche e i Nuovi Media sono entrati a far parte della vita quotidiana della maggior parte dei preadolescenti e degli adolescenti italiani, condizionandone abitudini e stili di vita, supportando e facilitando la comunicazione e, potenzialmente, la collaborazione. Rappresentano uno strumento che partecipa alla conquista della consapevolezza di sé e del controllo sulle proprie scelte, decisioni e azioni, un veicolo "nativo" di espressione e partecipazione.

La partecipazione basata sulle Tecnologie dell'Informazione e della Comunicazione deve essere collocata nel quadro dei diritti dei bambini e dei ragazzi, che comprendono la parità di accesso, la trasparenza, il diritto alla privacy, la libertà di espressione. Bambini e ragazzi devono contemporaneamente essere tutelati nel loro diritto ad essere protetti da abusi e violenze (artt. 19-34 della Convenzione ONU sui diritti dell'infanzia, CRC).

1.1 Scopo della Policy.

La presenza sempre più diffusa di tecnologie digitali anche all'interno degli ambienti scolastici pone in essere nuove necessità e attenzioni relative al loro uso sicuro, consapevole e positivo, in particolare per quanto riguarda l'uso di nuove tecnologie nella didattica e l'implementazione e la diffusione della rete internet (via cavo e Wi-Fi).

La comunità scolastica nel suo complesso è chiamata a svolgere un ruolo fondamentale nel garantire che bambini/e e adolescenti siano in grado di utilizzare le tecnologie digitali in modo appropriato e sicuro.

E' in questo quadro che s'inserisce la necessità di affrontare la questione da più punti di vista coinvolgendo più interlocutori al fine di dotare la nostra comunità scolastica di una propria Policy di E-safety che definisca:

1. misure atte a facilitare e promuovere l'utilizzo positivo delle Tecnologie dell'Informazione e della Comunicazione (T.I.C.) nella didattica e negli ambienti scolastici;
2. misure di prevenzione e di gestione di situazioni problematiche relative all'uso delle tecnologie digitali.

L'E-Safety dell'Istituto fa quindi riferimento a un insieme di regolamenti, linee di azione e attività che verranno poste in essere per fare fronte ad una serie di necessità individuate e che andranno ad integrarsi con gli altri regolamenti d'istituto e le politiche relative ai comportamenti degli alunni.

1.2 Ruoli e Responsabilità della Comunità Scolastica

Il ruolo del **Dirigente Scolastico** nel promuovere l'uso consentito delle tecnologie e di internet include i seguenti compiti:

- garantire la sicurezza (tra cui la sicurezza on-line) dei membri della comunità scolastica;
- garantire che tutti gli insegnanti ricevano una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze, un utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della Comunicazione (TIC);
- garantire l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line;
- seguire le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola.

Il ruolo dell'**Animatore digitale** include i seguenti compiti:

- stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornire consulenza e informazioni al personale in relazione ai rischi on-line e alle misure di prevenzione e gestione degli stessi;
- monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, nonché proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;
- accertarsi che gli utenti possano accedere alla rete della scuola e che questa sia dotata di appositi filtri di navigazione; curare lo sviluppo del sito web della scuola per scopi istituzionali e consentiti (istruzione e formazione);
- coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti la "scuola digitale".

Il ruolo del **Direttore dei Servizi Generali e Amministrativi** include i seguenti compiti:

- assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni;
- garantire il funzionamento dei diversi canali di comunicazione della scuola (sportello, circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet;
- assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente.

Il ruolo del **Personale Docente** e di ogni **figura educativa che lo affianca** include i seguenti compiti:

- informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;
- garantire che le modalità di utilizzo corretto e sicuro delle TIC e di internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;
- garantire che gli studenti capiscano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet;
- assicurare che gli studenti abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete, ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore;
- garantire che le comunicazioni digitali dei docenti con studenti e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali;
- assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, altri device da parte degli studenti durante le lezioni e ogni altra attività scolastica ove prevista e consentita;
- nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;

- comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
- segnalare qualsiasi problema o proposta di carattere tecnico-organizzativo ovvero esigenza di carattere informatico all'Animatore digitale ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC;
- segnalare al Dirigente scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli studenti in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dalle norme.

Il ruolo del **Personale ATA** include i seguenti compiti:

- avere adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto e relative buone pratiche;
- segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico o all'animatore digitale;
- mantenere tutte le comunicazioni digitali con studenti e genitori/tutori a livello professionale e realizzarle esclusivamente con sistemi ufficiali scolastici;

Il ruolo degli **studenti** include i seguenti compiti:

- essere responsabili, in relazione al proprio grado di maturità e di apprendimento, per l'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;
- prendere coscienza delle potenzialità offerte dalle Tecnologie dell'Informazione e della Comunicazione (TIC) per la ricerca di contenuti e materiali ma anche della necessità di evitare il plagio e rispettare i diritti d'autore;
- comprendere l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi;
- adottare condotte rispettose degli altri anche quando si comunica in rete;
- esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori.

Il ruolo dei **genitori** degli studenti include i seguenti compiti:

- sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle tecnologie dell'Informazione e delle Comunicazioni nella didattica;
- Seguire gli studenti nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllare l'utilizzo del pc e di internet;
- concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di internet;
- fissare delle regole per l'utilizzo del computer e tenere sotto controllo l'uso che i figli fanno di internet e del telefonino in generale.
- fare un uso appropriato delle immagini e video digitali acquisiti in occasione di eventi scolastici, anche al di fuori delle aule; dell'accesso alle sezioni del sito dedicate ai genitori, con particolare riguardo al registro elettronico.

1.3 Condivisione e comunicazione della policy all'intera comunità scolastica.

Per far sì che si diffonda fra tutti i membri della comunità scolastica un corretto uso delle TIC e della rete e per diffondere consapevolezza su norme e sanzioni, l'E-Safety Policy verrà condivisa con l'intera comunità scolastica avvalendosi di diversi mezzi:

Personale docente e Ata:

- Comunicazioni interne/circolari.
- Informazione e discussione al Collegio Docenti.
- Pubblicazione sul Sito Web d'Istituto nei Regolamenti.
- Distribuzione di una copia di E-Safety Policy in ogni plesso per la libera consultazione.

Studenti:

- Affissione in ogni aula delle regole per l'accesso a Internet anche con dispositivi personali.
- Discussione della E-Safety Policy in classe (scuola primaria e secondaria I°).
- Inserimento estratto E-Safety Policy d'istituto nel diario scolastico.
- Distribuzione di una copia di E-Safety Policy in ogni plesso per la libera consultazione.

Genitori:

- Pubblicazione della versione integrale della E-Safety Policy sul sito web d'istituto.
- Inserimento dell'E-Safety Policy nel diario di ogni alunno.
- Condivisione con le famiglie dell'adozione di questo nuovo regolamento nelle riunioni d'inizio anno.

1.4 Gestione delle infrazioni alla Policy.

Le infrazioni alla policy possono essere rilevate da docenti/ATA nell'esercizio delle proprie funzioni oppure possono essere segnalate da alunni e genitori a docenti/ATA.

Infrazioni al regolamento d'Istituto, utilizzo non permesso e inadeguato del cellulare o altro device.

Mancanza Disciplinare	Frequenza	Provvedimento	Organo
Lo studente usa il cellulare senza il consenso del docente.	a) 1° volta	Nota sul diario, ritiro del cellulare, consegna allo studente alla fine delle lezioni e colloquio con i genitori.	Docente Dirigente Scolastico o suo collaboratore.
	b) dalla 2° Volta in poi	Nota sul registro di classe, ritiro del cellulare e consegna alla fine delle lezioni. Colloquio con lo studente e i genitori. Provvedimento del Dirigente di richiamo scritto con assegnazione di eventuali attività socialmente utili da svolgere a scuola. Per infrazioni reiterate, sospensione dalle lezioni per uno o più giorni. Ricadute sul voto di comportamento.	Docente Dirigente Scolastico Consiglio di classe Consiglio di Istituto
Lo studente utilizza il cellulare o altro dispositivo. Lo studente acquisisce in ambito scolastico, con il cellulare o con altro dispositivo, dati personali (immagini, suoni, filmati) e li diffonde nella rete o a terzi, senza autorizzazione dei diretti interessati.		Nota sul registro di classe, ritiro del cellulare e consegna alla fine delle lezioni. Colloquio con lo studente e i genitori. Provvedimento del Dirigente di richiamo scritto con assegnazione di eventuali attività socialmente utili da svolgere a scuola. Per infrazioni reiterate, sospensione dalle lezioni per uno o più giorni. Ricadute sul voto di comportamento.	Docente Dirigente Scolastico Consiglio di classe Consiglio di Istituto

Qualora esse si configurino come vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso. Infatti è bene ricordare a tutti che nel momento in cui un qualunque attore della comunità scolastica venga a conoscenza di un reato perseguibile d'ufficio, è fatto obbligo di denuncia (ex art. 331 del codice di procedura penale).

L'omissione di denuncia costituisce reato (art. 361). I reati che, in ambiente scolastico, possono essere riferiti all'ambito digitale e commessi per via telematica sono tra gli altri:

- Minaccia, in particolare, se la minaccia è grave, per tale reato si procede d'ufficio (art. 612 codice penale).
- Induzione alla prostituzione minorile (art. 600bis).
- Pedopornografia (art. 600ter).
- Corruzione di minorenni (art. 609quinqüies).

Per i reati sessuali la magistratura di norma procede su querela di parte; tuttavia nei casi più gravi si persegue d'ufficio e in genere i reati verso le/i minori sono tra quelli per i quali si procede d'ufficio.

Nel caso in cui le infrazioni della policy violino norme previste dal Regolamento di Istituto si procede secondo quanto previsto dal Regolamento stesso; qualora le infrazioni riguardino l'opportunità di certi comportamenti o la convivenza civile, la scuola eroga delle sanzioni secondo il principio della sensibilizzazione e del risarcimento dell'eventuale danno provocato, in uno spirito di recupero e rieducazione.

La realizzazione di quanto esposto è supportata dalla partecipazione dell'Istituto Comprensivo Ilaria Alpi di Torino al progetto di Educazione alla legalità, i cui attori sono, oltre alle scuole, la Polizia Municipale di Torino - Nucleo di Prossimità, la Polizia Postale (interventi del progetto “#CUORICONNESSI”).

1.5 Monitoraggio dell'implementazione della Policy e suo aggiornamento.

La Policy verrà monitorata dalla Dirigenza, dall'Animatore Digitale, dai referenti di plesso della commissione informatica e verrà revisionata e aggiornata ogni anno alla luce delle esigenze emerse.

1.6 Integrazione della Policy con Regolamenti esistenti.

La policy verrà integrata con il regolamento d'istituto e il patto educativo in vigore.

2. Formazione e Curricolo

2.1. Curricolo sulle competenze digitali per gli studenti.

La competenza digitale fa riferimento alla capacità di comprendere e sfruttare l'effettivo potenziale delle tecnologie in ottica di costruzione di conoscenza e di promozione della partecipazione e dell'inclusione; il rapporto con le tecnologie digitali guarda così a forme di uso consapevole, critico e creativo.

Nella scuola primaria attraverso la disciplina “tecnologia” si può promuovere l'integrazione delle conoscenze teoriche con quelle pratiche che concorrono alla comprensione di sistemi complessi.

Nella scuola secondaria di primo grado la competenza digitale è annoverata ancora tra le competenze trasversali necessarie alla cittadinanza; non è previsto un curriculum specifico ed unitario dedicato ai linguaggi medialità e alla competenza digitale, ma solamente il riferimento a obiettivi di apprendimento e traguardi di competenze nelle diverse aree disciplinari.

Allo stato attuale quindi la competenza digitale va a configurarsi non come disciplina autonoma, ma come ambito che gli studenti possono sviluppare in maniera trasversale nel complesso delle attività didattiche.

Si sottolinea, inoltre, che, per quanto riguarda le tecnologie dell'informazione e della comunicazione e le tecnologie digitali, oltre alla padronanza degli strumenti, è necessario sviluppare un atteggiamento critico ed una consapevolezza rispetto agli effetti sociali e culturali della loro diffusione, alle conseguenze relazionali e psicologiche dei possibili modi d'impiego, alle ricadute di tipo ambientale o sanitario. Si riconosce che quest'ultimo compito educativo, in particolare, deve essere condiviso tra tutte le discipline.

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

Il concreto utilizzo delle Tic in classe come elemento innovativo non dipende solamente dall'effettiva e funzionale dotazione strumentale, ma anche e soprattutto dalla capacità di comprenderne le potenzialità rispetto a contesti e finalità specifici. Per sostenere un processo di consapevole innovazione didattica è necessario investire sulla formazione e l'aggiornamento degli insegnanti. La nostra scuola supporterà la formazione dei docenti in servizio attraverso:

- L'organizzazione di corsi interni sulle tematiche emerse dal questionario sul "Piano di attuazione del PNSD".
- La partecipazione a reti di scuole che effettuano anche percorsi di formazione.
- La diffusione tramite sito web d'informazioni su corsi sia gratuiti sia a pagamento organizzati da diversi enti .

Nel corso degli anni alcuni docenti dell'Istituto hanno partecipato a corsi su:

- Piano di formazione Nazionale sulle TIC percorsi a e b.
- Utilizzo delle LIM in classe.
- Uso delle tecnologie per la didattica.
- Pensiero computazionale – Coding .

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

L'implementazione della rete internet nella scuola - in particolare il wifi - renderà ancor più pressante la necessità di formare i docenti sull'uso consapevole di internet e sui rischi della rete. L'Istituto prevede la formazione e l'aggiornamento dei docenti in tal senso attraverso:

- l'organizzazione di corsi interni;
- la partecipazione a reti di scuole che effettuano anche percorsi di formazione (cyberbullismo);
- la diffusione tramite sito web di informazioni su corsi sia gratuiti sia a pagamento organizzati da diversi enti;
- la partecipazione alla piattaforma Generazioni Connesse.

2.4 Sensibilizzazione delle famiglie.

Gli adulti devono assicurare l'opportunità a bambini e ragazzi di utilizzare in modo sicuro e consapevole i nuovi media, ed è proprio a tal fine che l'istituto organizza da anni incontri di sensibilizzazione aperti alle famiglie, anche con la collaborazione di associazioni del territorio, Polizia Municipale - Nucleo di Prossimità e della Polizia Postale. Gli incontri si strutturano in dimostrazioni/lezioni con esperti del settore in cui vengono forniti suggerimenti per l'uso di Internet e delle tecnologie.

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

3.1 Accesso ad internet: filtri, antivirus e sulla navigazione.

Al momento della stesura del presente documento (a.s. 2017-2018) i plessi della scuola primaria sono in fase di allacciamento attraverso la fibra Ottica (OpenFibra) come previsto dal progetto "Ri-Conessioni in corso" della Fondazione per la scuola della Compagnia di San Paolo. Al termine dei lavori le connessioni saranno a banda larga filtrata come programmato.

La scuola dell'Infanzia Perempruner ha, ad oggi, un solo PC connesso alla rete e destinato all'utilizzo dei soli insegnanti. La scuola secondaria di primo grado B. Croce possiede al momento una rete wifi con connessione a banda larga via etere Garr - gestione CSP - che comprende di un servizio centralizzato di URL Filtering, basato sulla piattaforma Asso Dschola (blacklist dell'Università di Tolosa) che permette di bloccare l'accesso a pagine web appartenenti a categorie non adatte all'ambiente scolastico (Es: pornografia, contenuti violenti, gioco d'azzardo, peer to peer, ecc...).

Nei laboratori destinati agli allievi della Scuola Secondaria, e nel PC presente in ogni classe e connesso al Web attraverso la Rete protetta Garr, il sistema operativo installato è una distribuzione GNU/Linux, (Edubuntu) allo scopo di ridurre al minimo i costi delle licenze acquistate dalla scuola, formare gli allievi all'uso di prodotti open source, fornire una maggiore protezione da infezioni di virus.

3.2 Gestione accessi (password, backup, ecc.).

La connessione ad internet della scuola ha un proprio utente e password univoci di accesso. Il personale ha la responsabilità di mantenere questi dati privati. Agli allievi non vengono fornite queste informazioni.

3.3. E-mail.

E' in fase di studio la possibilità di fornire a tutto il personale docente e ata una casella di posta elettronica avente il dominio @icilariaalpitorino.gov.it per le seguenti finalità:

- permettere comunicazioni tra il personale scolastico, le famiglie e gli studenti via e-mail in quanto queste devono avvenire preferibilmente tramite un indirizzo ufficiale e-mail della scuola;
- per consentire l'attivazione di protocolli di controllo all'interno di piattaforme di apprendimento;
e con le seguenti regole:
 - gli utenti si impegnano a non diffondere informazioni che possono nuocere alla reputazione della scuola o essere contrarie alla morale o alle leggi in vigore. Ogni messaggio trasmesso deve recare il nome del suo autore. Non è consentita la pubblicità, in nessuna forma.
 - la mail d'istituto deve utilizzata solamente per comunicazione di carattere lavorativo;
 - E-mail in arrivo da mittenti sconosciuti vanno trattate come sospette ed eventuali allegati non devono essere aperti;

3.4 Blog e sito web della scuola.

Il Dirigente, o persona da questi delegata, si assume la responsabilità di assicurare che:

- il contenuto del sito sia preciso e la qualità della presentazione sia mantenuta;
- il caricamento delle informazioni sul sito sia compito esclusivo dell'autorità delegata a tale compito; il sito web della scuola sia conforme alle linee guida di legge;
- la maggior parte del materiale è frutto del lavoro della scuola; qualora fosse pubblicato il lavoro di altri verranno rese note le fonti utilizzate e indicata chiaramente l'identità dell'autore;

- i contatti indicati sul sito web siano: l'indirizzo della scuola, il numero di telefono, l'email; le foto pubblicate sul web non abbiano un nome completo in allegato;
- non siano usati i nomi degli alunni quando si salvano le immagini nei nomi dei file o dei tag durante la pubblicazione sul sito web della scuola;

Gli utenti stessi (cfr. Legge sul diritto d'autore, LDA, del 9 ottobre 1992) e nei singoli casi si impegnano a menzionare le fonti quando si servono di informazioni di terze persone:

- si impegnano a non diffondere informazioni che appartengono a terzi senza l'autorizzazione degli stessi (cfr. Legge sul diritto d'autore, LDA, del 9 ottobre 1992) e nei singoli casi si impegnano a menzionare le fonti quando si servono di informazioni di terze persone.

Sono proibite la duplicazione e la diffusione di programmi e documenti coperti dal diritto d'autore.

3.5 Social network.

L'istituto comprensivo per il momento non si avvale dell'uso di social network.

3.6 Protezione dei dati personali.

Si fa riferimento a tutto quanto previsto dal Decreto legislativo 30 giugno 2003, n. 196 (c.d. Codice della Privacy). Tuttavia, si possono individuare al riguardo alcune linee guida di e-safety:

- il personale non deve condividere numeri di telefono personali o indirizzi di posta elettronica privati con la componente studentesca e con i genitori.

Un telefono o una e-mail della scuola sarà fornito al personale cui è richiesto il contatto con la componente studentesca o con i genitori.

- Le fotografie o i video da pubblicare sul sito che includano allieve e allievi saranno selezionati con cura e non permetteranno a singoli di essere chiaramente identificati a meno che non si tratti di eventi particolari per cui le famiglie potranno concedere opportuna autorizzazione. La scuola cercherà di utilizzare fotografie o video di gruppo piuttosto che foto integrali di singoli.

- I nomi completi di alunne e alunni saranno evitati sul sito web come pure nei blog, forum e wiki, in particolare se in associazione con le loro fotografie.

- All'atto dell'iscrizione è richiesto alle famiglie di firmare un'autorizzazione scritta per consentire l'uso didattico di immagini e video delle/dei minori secondo i principi sopra indicati.

- Ogni caso particolare sarà preso in considerazione per stabilire l'opportunità di pubblicare dati personali e sarà presentata apposita richiesta circostanziata che varrà solo per lo specifico evento.

4. Strumentazione personale.

4.1 Gestione degli strumenti personali.

- Studenti.

I telefoni cellulari, i tablet e le relative fotocamere e registratori vocali non verranno utilizzati durante le lezioni scolastiche se non all'interno di attività didattiche espressamente programmate dal corpo docente.

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, prima dell'appello, gli allievi devono disattivare i propri telefonini (se posseduti perchè ritenuti indispensabili alle comunicazioni con gli adulti autorizzati dalla famiglia e utilizzabili al di fuori dall'edificio scolastico) e custoditi con attenzione all'interno dello zaino, della propria cartella.

L'istituto non risponde di eventuali danneggiamenti e furti dei dispositivi personali.

Studenti con disturbi specifici di apprendimento, previa consultazione con il Consiglio di Classe, concorderanno le modalità di impiego di strumenti compensativi quali tablet e computer portatili e le modalità di custodia nell'armadietto della classe.

Giochi e console, tra cui la Sony Playstation, Microsoft Xbox, Nintendo e similari, che possono avere accesso a Internet non filtrato, non sono consentiti nemmeno se custoditi dentro gli zaini, le borse personali. Saranno requisiti dal docente che ravvisa l'infrazione, depositati nella cassaforte della segreteria e consegnati al genitore/tutore convocato, che sarà contestualmente informato dell'eventuale sanzione disciplinare comminata al trasgressore.

Nel caso in cui debbano comunicare con la famiglia durante l'orario scolastico, alunne e alunni, allieve ed allievi possono usare gratuitamente la linea fissa della scuola rivolgendosi a un operatore; allo stesso modo le famiglie devono chiamare il centralino della scuola se hanno assoluta necessità di parlare con i propri figli. Si raccomanda di ridurre tali comunicazioni a casi di inderogabile necessità e urgenza.

L'invio di materiali abusivi, offensivi o inappropriati è vietato, anche se avviene all'interno di cerchie o gruppi di discussione privati.

- Personale docente.

Il personale preferirà, quando ciò è possibile, l'impiego della strumentazione fornita dalla scuola rispetto a quella personale (portatili, pc fissi, ...); le infrastrutture e gli apparati della scuola non vanno utilizzati per scopi personali. Telefoni cellulari, tablet, fotocamere e altri strumenti di registrazione audio/video non devono essere impiegati durante le lezioni scolastiche se non all'interno di attività didattiche espressamente programmate.

La password di accesso alla rete wireless va custodita con cura e per nessuna ragione deve essere divulgata a chi non ha titolo per utilizzarla (studenti, genitori, operatori esterni). L'uso improprio della rete è contestato al titolare delle credenziali con cui è avvenuta la comunicazione.

Qualora si utilizzino a scuola dispositivi di archiviazione esterna di proprietà personale (chiavette usb, dischi fissi portatili) è bene controllare preventivamente che essi siano esenti da virus per evitare di danneggiare le attrezzature comuni.

Durante l'attività didattica è opportuno che ogni insegnante:

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

L'uso improprio di dispositivi personali (smartphone, tablet) o della strumentazione informatica della scuola, verrà sanzionato in base alla normativa vigente.

- Collaboratori scolastici

Fatti salvi i momenti di pausa, ai collaboratori scolastici non è consentito in alcun modo l'uso di strumenti tecnologici personali (pc portatili, tablet, smartphone, e-reader, cellulari....). L'uso improprio verrà sanzionato in base alla normativa vigente.

5. Prevenzione, rilevazione e gestione dei casi.

Prevenzione:

I docenti svolgeranno attività di formazione/informazione in classe adeguando le attività all'età degli alunni e avvalendosi di materiali di supporto, fra cui anche quelli messi a disposizione da "Generazioni Connesse".

La prevenzione passa poi anche attraverso percorsi di educazione all'affettività e all'emozionalità che già si svolgono in istituto. In collaborazione con associazioni del territorio, enti preposti (Polizia Municipale e Postale) si attueranno anche attività di sensibilizzazione alle famiglie. In particolare le attività si concentreranno sull'analisi dei rischi in rete maggiormente diffusi:

- Cyberbullismo (bullismo attraverso strumenti telematici).
- Sexiting (testi, video, immagini inerenti alla sessualità).
- Grooming (adescamento di minore).

Azioni:

Le azioni d'intervento del personale scolastico andranno ad agire su più piani:

1. Rilevazione

Le azioni verranno intraprese a seguito di:

- segnalazioni da parte degli alunni o delle famiglie;
- segnalazioni durante gli incontri con gli esperti;
- segnalazioni su sportello virtuale.

2. Segnalazione

Il docente che riceve la segnalazione deve provvedere a informare il consiglio di classe e il collaboratore del dirigente che provvederà ad informare il Dirigente.

3. Gestione dei casi

Il Dirigente scolastico e/o il Consiglio di classe hanno la possibilità di sostituire le sanzioni disciplinari più severe con altri provvedimenti, comprendenti la collaborazione ai servizi interni della scuola o altre attività a scopo sociale che possono utilmente costituire una riparazione ed un ammonimento, quali:

- cooperazioni di pulizia e ripristino degli arredi dei locali scolastici;
- collaborazione con il personale ausiliario;
- riordino della biblioteca e/ o dei laboratori;
- ricerche e/o attività di studio ed approfondimento coerenti con l'infrazione commessa.

Prevenzione, rilevazione e gestione

R I S C H I	A Z I O N I
Adescamento online (grooming).	Sensibilizzazione sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni e per indurli alla prostituzione. Qualora si venga a conoscenza di casi simili, occorre valutarne la fondatezza e avvisare il Dirigente Scolastico per l'intervento delle forze dell'ordine.
Cyberbullismo.	Campagne di sensibilizzazione e informazione anche con l'ausilio di progetti e realtà esterni. I casi possono essere molto variegati, variando dal semplice scherzo di cattivo gusto via sms/Whatsapp a vere e proprie minacce verbali e fisiche, che costituiscono reato. Occorre confrontarsi con il Dirigente Scolastico sulle azioni da intraprendere.
Dipendenza da Internet, videogiochi, shopping o gambling online (gioco d'azzardo)...	Informazioni sul fatto che ciò può rappresentare una vera e propria patologia che compromette la salute e le relazioni sociali e che in taluni casi (per es. uso della carta di credito a insaputa di altri) rappresenta un vero e proprio illecito.
Esposizione a contenuti pornografici, violenti, razzisti, ...	Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale della navigazione e sensibilizzazione sulla necessità di monitorare l'esperienza online dei propri figli. Verso alunni e allievi: inserimento nel curriculum di temi legati alla affidabilità delle fonti online, all'interculturalità e al rispetto delle diversità. Qualora si venga a conoscenza di casi simili, occorre convocare i genitori per richiamarli a un maggiore controllo sulla fruizione di Internet da parte dei propri figli e/ o sulla necessità di non usufruirne in presenza degli stessi.
Sexting e pedopornografia.	Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale della navigazione. Verso la componente studentesca: inserimento nel curriculum di temi legati all'affettività, alla sessualità e alle differenze di genere. In casi simili, se l'entità è lieve occorre in primo luogo parlarne con alunne e alunni e rispettivi genitori, ricordando loro che l'invio e la detenzione di foto che ritraggono minorenni in pose sessualmente esplicite configura il reato di distribuzione di materiale pedopornografico. Chi è immerso dalla nascita nelle nuove tecnologie spesso non è consapevole che una foto o un video diffusi in rete potrebbero non essere tolti mai più né è consapevole di scambiare o diffondere materiale pedopornografico. In casi di rilevante gravità occorre informare tempestivamente il Dirigente Scolastico per gli adempimenti del caso.
Violazione della privacy.	Informazione sull'esistenza di leggi in materia di tutela dei dati personali e di organismi per farle rispettare. Se il comportamento rilevato viola solo le norme di buona convivenza civile e di opportunità, occorre convocare i soggetti interessati per informarli e discutere dell'accaduto e concordare forme costruttive ed educative di riparazione. Qualora il comportamento rappresenti un vero e proprio illecito, il Dirigente Scolastico deve esserne informato in quanto a seconda dell'illecito sono previste sanzioni amministrative o penali.