

E-Safety Policy dell'Istituto Comprensivo Roberto Castellani

1. Introduzione

- Scopo della Policy

La presenza sempre più diffusa delle tecnologie digitali nella vita di tutti i giorni offre sicuramente nuove e grandi possibilità anche nel mondo della scuola, tuttavia ci impone una riflessione sul loro uso efficace, sicuro e consapevole. “Lo sviluppo e l'integrazione dell'uso delle TIC, ed in particolare di internet, nella didattica, offrono le condizioni e l'occasione per una trasformazione dell'insegnamento e dell'apprendimento nelle scuole, ma ci mette di fronte a sfide importanti, che riguardano più livelli di conoscenze, abilità e attitudini che i più giovani hanno bisogno di sviluppare, nell'ottica di accrescere le competenze digitali” (tratto dal sito: www.generazioniconnesse.it)

Questa *Policy* si applica a tutti i membri della comunità scolastica che hanno accesso o che sono utenti dei sistemi informatici dell'Istituto Comprensivo Roberto Castellani.

In particolare l'intento della scuola è quello di promuovere l'uso consapevole e critico da parte degli alunni delle tecnologie digitali e di internet, di far acquisire loro procedure e competenze “tecniche” ma anche corrette norme comportamentali, di prevenire ovvero rilevare e fronteggiare le problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso, delle tecnologie digitali.

L'Istituto Comprensivo Roberto Castellani accoglie minori “nativi digitali” che fin dall'infanzia sono esposti a rischi di cui sono inconsapevoli, pertanto la scuola attua parallelamente attività di prevenzione, controllo e formazione di allieve, allievi e famiglie allo scopo di ridurre al minimo l'occorrenza di atti che non solo creano disagio nella comunità scolastica, ma possono configurarsi come reati.

Il presente documento descrive perciò

- le misure atte a facilitare e promuovere l'utilizzo delle TIC nella didattica sviluppando le competenze digitali
- le norme comportamentali e le procedure per l'utilizzo delle TIC
- le misure per la prevenzione e quelle per la rilevazione e gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali

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

Gli adulti hanno un ruolo fondamentale nel garantire che gli adolescenti siano in grado di utilizzare le tecnologie digitali e che lo facciano in modo appropriato e sicuro, ruolo che vede coinvolti a pieno titolo tutti coloro che hanno un ruolo educativo, oltre che formativo, primi fra tutti i genitori e la comunità scolastica nel suo complesso.

Non va tuttavia sottovalutato il ruolo degli studenti come primi attori del percorso di acquisizione della capacità di positiva gestione delle proprie competenze digitali: in tale ottica si rende indispensabile responsabilizzare e rendere attivi gli studenti nell'uso delle TIC.

1) Il Dirigente scolastico nel promuovere l'uso consapevole delle tecnologie e di internet

- cura la sicurezza on-line della comunità scolastica;
- favorisce la cultura dell'inclusione dell'altro/a e delle differenze, e l'utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della Comunicazione (TIC) , tramite incontri con il personale e la promozione/adesione a percorsi formativi e di autoformazione del personale docente, l'attivazione di progettualità dedicate per gli alunni.

2) Il Direttore dei servizi generali e amministrativi

- assicura, 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
- garantisce il funzionamento dei diversi canali di comunicazione della scuola (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 nell'ambito dell'utilizzo delle tecnologie digitali e di internet;

3) Animatore Digitale e Team dell'Innovazione

- Promuovono l'aggiornamento dei docenti
- Propongono e promuovono l'uso delle TIC

4) Docente Funzione strumentale per le nuove tecnologie

- cura il sito web della scuola per scopi istituzionali e consentiti;
- supporta l'attività laboratoriale con consigli, aiuti e chiarimenti;
- monitora l'utilizzo delle TIC e segnala al DSGA eventuali problemi che dovessero richiedere acquisti o interventi tecnici;
- assicura che il personale possa accedere alla rete della scuola solo tramite password;
- ha il compito di assicurare che l'e-Safety sia a conoscenza di tutto il personale;
- fornisce al personale, agli alunni e ai genitori consulenza e informazioni in relazione ai rischi on line e alle misure di prevenzione e gestione degli stessi;
- riceve segnalazioni di incidenti e-Safety e *crea un registro degli incidenti* e informa il DS

5) Docenti:

- illustrano ai propri allievi le regole di utilizzo contenute nel presente documento;
- danno chiare indicazioni sul corretto utilizzo della strumentazione multimediale, di internet, ecc.;
- segnalano prontamente eventuali malfunzionamenti o danneggiamenti al docente funzione strumentale;
- non divulgano le credenziali di accesso alla rete wifi;
- non salvano sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili;
- si informano/si aggiornano sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;
- garantiscono che gli alunni capiscano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet;
- controllano l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito);
- nelle lezioni in cui è programmato l'utilizzo di Internet, guidano gli alunni a siti controllati e verificati come adatti per il loro uso e controllano che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;

- segnalano al Dirigente Scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dalle norme.

6) Il Personale ATA è tenuto a:

- avere adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto e relative buone pratiche;
- aver letto, compreso e sottoscritto la presente policy;
- segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico o ai suoi collaboratori o alla Funzione Strumentale per le nuove tecnologie o all'Animatore Digitale per le opportune indagini / azioni / sanzioni;

7) Gli studenti devono:

- utilizzare le TIC su indicazioni del docente;
- in caso di riscontro di malfunzionamenti della strumentazione e/o di contatto accidentale con informazioni, immagini e/o applicazioni inappropriate comunicarlo immediatamente all'insegnante;
- non eseguire tentativi di modifica della configurazione di sistema delle macchine;
- non utilizzare la strumentazione della scuola a scopi personali, ludici e/o ricreativi (a meno che l'attività didattica non lo preveda esplicitamente);
- non utilizzare propri dispositivi esterni personali senza aver acquisito il permesso da parte dell'insegnante;
- chiudere correttamente la propria sessione di lavoro;
- archiviare i propri documenti in maniera ordinata e facilmente rintracciabile in una cartella personale (con il proprio nome e classe) creata all'interno della cartella documenti dell'account loro destinato;
- essere consapevoli dei problemi di sicurezza connessi con l'uso di telefoni cellulari, telecamere e dispositivi portatili;
- essere responsabili dell'utilizzo delle attrezzature tecnologiche della scuola e comprendere l'importanza di adottare buone pratiche di e-Safety anche quando utilizzano tecnologie digitali fuori dalla scuola

7) I genitori hanno 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 alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllare l'utilizzo del pc e di internet;
- concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di internet;
- fissare delle regole per l'utilizzo del computer e tenere sotto controllo l'uso che i figli fanno di internet e del telefonino in generale.

- Condivisione e comunicazione della *policy* all'intera comunità scolastica.

Il presente documento sarà oggetto di condivisione e revisione da parte dell'intera comunità scolastica con il coinvolgimento di studenti, docenti e famiglie, con l'approvazione degli organi collegiali.

Di esso viene data ampia diffusione a tutta la comunità scolastica, attraverso la pubblicazione sul sito web istituzionale.

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. A partire dalla pubblicazione sul sito della scuola, si possono ipotizzare per esempio:

- per il corpo docente un confronto collegiale, su base annuale, circa la necessità di apportare modifiche e miglioramenti alla *policy* vigente ed elaborazione di protocolli condivisi di intervento;
- per gli alunni, la discussione in classe della *policy* nei primi giorni di scuola, con particolare riguardo alle nuove classi prime;
- 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.

- Gestione delle infrazioni della *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.

- Monitoraggio dell'implementazione della Policy e suo aggiornamento

Il monitoraggio dell'implementazione della Policy verrà curata dal DS in collaborazione con la Funzione Strumentale, l'Animatore Digitale e il Team dell'Innovazione che promuoveranno inoltre gli eventuali aggiornamenti che si rendano opportuni, secondo una logica di condivisione con tutto il corpo docente e le famiglie.

- Integrazione della Policy con documenti esistenti

Il presente documento si integra pienamente con obiettivi e contenuti dei seguenti documenti: PTOF, POF, Regolamento d'Istituto, Patto Educativo di corresponsabilità, Regolamento di accesso e utilizzo delle postazioni multimediali

2. FORMAZIONE E CURRICOLO

- Curricolo sulle competenze digitali per gli studenti

La raccomandazione 2006/962/CE del Parlamento Europeo e del Consiglio dell'Unione Europea individua il quadro di riferimento europeo in materia di competenze chiave per l'apprendimento permanente. Tra queste è citata la competenza digitale, ovvero il "saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione (TSI) per il lavoro, il tempo libero e la comunicazione".

Al fine di promuovere l'acquisizione e l'incremento delle competenze digitali, verranno svolte attività dirette a perseguire i seguenti obiettivi:

1. conoscere e acquisire consapevolezza su natura, ruolo e opportunità delle TSI nella vita quotidiana e professionale;
2. distinguere il reale dal virtuale e riconoscerne le correlazioni e le conseguenze delle correlazioni;
3. sviluppare le abilità di base nelle TSI (saper usare il computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni);
4. usare le informazioni in modo critico, accertandone la provenienza e l'affidabilità;
5. acquisire consapevolezza su come le TSI possono coadiuvare la creatività e l'innovazione;
6. riflettere sulle problematiche legate alla validità e all'affidabilità delle informazioni disponibili;

7. acquisire consapevolezza sulle opportunità e sui potenziali rischi di Internet e della comunicazione tramite i supporti elettronici;
8. riflettere sui principi giuridici ed etici di base che si pongono nell'uso interattivo delle TSI (netiquette, privacy...).

In virtù della valenza trasversale delle competenze digitali, la loro acquisizione è promossa attraverso percorsi didattici disciplinari e/o interdisciplinari inerenti diverse aree, coerentemente con gli obiettivi individuati nel Curricolo di Istituto e nelle programmazioni individuali.

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

Un gruppo di docenti dell'istituto nel corso dell' a.s. 2015/16 ha partecipato a corsi di formazione nell'ambito del piano nazionale scuola digitale organizzati dalla rete RISPO di Prato e/o on line (es. Coding in your classroom now) ed 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 e il supporto dell'Animatore Digitale, la partecipazione alle iniziative promosse dall'Amministrazione centrale e dalle scuole polo e a corsi di aggiornamento online.

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

I docenti dell'istituto Roberto Castellani hanno partecipato al corso di formazione legato al progetto "Generazioni connesse" e dall' a.s. 2012/13 sono organizzati incontri di formazione sull'uso responsabile e sicuro delle nuove tecnologie, in particolare di internet (accesso a facebook e social network in genere da parte dei minori, rispetto delle regole nel mondo virtuale della rete ecc.) con agenti della Polizia Postale. Tali incontri sono stati aperti anche a i genitori

- Sensibilizzazione delle famiglie

Come detto al paragrafo precedente, dall' a.s. 2012/13 sono organizzati incontri di formazione sull' uso responsabile e sicuro delle nuove tecnologie con agenti della Polizia postale, aperti anche ai genitori.

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 ICT DELLA SCUOLA.

L'infrastruttura e la strumentazione ICT dell'Istituto sono un patrimonio di tutti, esse vanno utilizzate nel rispetto delle norme contenute nel "Regolamento di accesso e utilizzo delle postazioni multimediali". I danni causati alle attrezzature saranno a carico di chiunque disattenda il suddetto Regolamento.

L'accesso ad infrastrutture e strumentazione ICT utilizzabili per la didattica è riservato agli insegnanti e agli alunni ed è limitato al perseguimento di scopi formativi. I docenti devono formare i propri alunni al rispetto del suddetto Regolamento, per gli aspetti di loro pertinenza.

[L'Istituto è dotato di una rete wireless nei plessi della scuola secondaria e della scuola primaria](#)

Accesso a internet e navigazione

L'accesso a internet è consentito a scopi didattici al personale docente attraverso l'assegnazione di una password comune a tutti. Agli alunni è permessa la navigazione in internet dai pc del laboratorio o delle aule collegate alle LIM sotto il diretto controllo dei docenti che non devono mai comunicare la password di accesso.

Back up

Non vi è un backup dei file elaborati, se non quello operato dai docenti interessati sui supporti rimovibili personali. Le postazioni del laboratorio funzionano come stazioni di lavoro e non come archivi.

E-mail.

L'account di posta elettronica istituzionale è quello fornito dal Ministero dell'Istruzione dell'Università e della Ricerca, sia nella versione posta ordinaria che certificata. Questi account sono utilizzati ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita: l'invio o ricevimento di posta a scopi didattici avviene su autorizzazione del DS e operativamente è svolto dall'assistente amministrativo addetto. Ogni dipendente è dotato di posta elettronica ordinaria del dominio *castellani.prato.gov.it*. La casella di posta elettronica è di tipo "aziendale" e non può essere utilizzata per scopi personali. Sono attivati gruppi di discussione per ordine di scuola e per plesso. La funzionalità dei gruppi di discussione serve per consentire un rapido scambio di informazioni, opinioni, documenti tra colleghi e incentivare la partecipazione di tutti i docenti alla vita scolastica. La policy di uso della casella di posta elettronica è dettagliatamente pubblicata sul sito dell'Istituto nella sezione "note legali". Le circolari, le informazioni principali, le convocazioni saranno diramate esclusivamente tramite posta elettronica.

Sito web della scuola.

La scuola attualmente ha un sito web. Tutti i contenuti del settore didattico sono pubblicati direttamente e sotto supervisione della Funzione Strumentale, che ne valuta con il Dirigente Scolastico la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy, ecc.

Social network.

Attualmente nella didattica non si utilizzano social network, né l'istituzione scolastica vi ha creato una pagina col proprio profilo o ha autorizzato il personale scolastico a utilizzarli per nome e per conto della stessa. *È possibile, in via sperimentale, utilizzare il prodotto "Classroom" fornito da Google ad ogni docente per attivare una didattica su classi digitali.*

Cloud storage

I docenti si avvalgono di alcuni software di cloud storage per condividere materiale didattico.

Registro elettronico.

Ogni famiglia riceve le credenziali per l'accesso riservato al registro elettronico, in cui il corpo docente è tenuto a registrare assenze, valutazioni, note e osservazioni. Tramite le stesse credenziali i genitori possono leggere le schede di valutazione di fine quadrimestre dei propri figli: coloro che non possono accedere a Internet e di conseguenza non possono consultare il registro elettronico possono rivolgersi alla segreteria didattica per stampare i documenti di valutazione di fine quadrimestre

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 su supporto cartaceo e su supporto informatico, ai fini della protezione e sicurezza degli stessi.

Viene inoltre fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori.

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 per la documentazione delle attività didattiche

4. STRUMENTAZIONE PERSONALE

Per gli alunni

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 e con il permesso dei docenti.

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 telefoni e altri dispositivi dentro una scatola appositamente collocata in classe e li recupera al termine delle lezioni.

Alunni con disabilità, con disturbi specifici di apprendimento, BES, 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.

In caso di violazione delle suddette disposizioni, sarà previsto il ritiro temporaneo dei dispositivi da parte del docente che rileva la violazione. Gli strumenti non permessi saranno consegnati al DS o ai suoi collaboratori e depositati nella cassaforte della segreteria e successivamente consegnati al genitore/tutore convocato, che sarà contestualmente informato dell'eventuale sanzione disciplinare comminata al trasgressore.

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 della presente Policy.

Nel caso in cui gli alunni debbano comunicare con la famiglia durante l'orario scolastico, possono usare gratuitamente la linea fissa della scuola rivolgendosi a un operatore autorizzati dai docenti; 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.

Per il personale docente/ATA.

Il personale preferirà, quando ciò è possibile, l'impiego della strumentazione fornita dalla scuola rispetto a quella personale (portatili, pc fissi, tablet...); le infrastrutture e gli apparati della scuola non vanno utilizzati per scopi personali. I docenti sono autorizzati ad utilizzare devices (tablet e notebook) personali in classe unicamente per fini didattici e professionali. In tal caso la responsabilità sulla conservazione e corretta gestione degli stessi è affidata unicamente al proprietario.

Telefoni cellulari, 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).

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

Tutto il personale scolastico è autorizzato ad utilizzare devices personali laddove non stia assolvendo ad un ruolo didattico, a condizione che l'utilizzo non intralci il normale svolgimento delle attività scolastiche, né distraiga dal corretto svolgimento delle proprie mansioni. In tal caso la responsabilità sulla conservazione e corretta gestione degli stessi è affidata unicamente al proprietario.

Nell'invitare tutta la comunità scolastica (studenti, docenti, personale ATA e famiglie) ad evitare, per quanto non necessario, la pubblicazione in rete di immagini e/o video ripresi all'interno dell'Istituto (fatta salva la pubblicazione a scopi didattici, previa informativa al Dirigente Scolastico), è bene ricordare che, secondo la normativa vigente, non si possono diffondere immagini, video o foto sul web se non con il consenso delle persone riprese e che la diffusione di filmati e foto che ledono la riservatezza e la dignità delle persone può far incorrere in gravi violazioni, incorrendo in sanzioni disciplinari, pecuniarie ed eventuali reati.

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

Prevenzione

Per i ragazzi nativi digitali le interconnessioni tra vita e tecnologia sono la normalità. Essi, pur essendo spesso tecnicamente competenti, tendono a non cogliere le implicazioni dei loro comportamenti e tale fenomeno è tanto maggiore quanto è più forte il coinvolgimento emotivo nell'utilizzo dei nuovi media.

Ciò fa sì che alcuni rischi che fanno parte del mondo digitale possano non essere percepiti come tali ed è dunque compito degli adulti, famiglie ed insegnanti, affrontarli con l'obiettivo di prevenirli.

Tra i principali rischi, sia di carattere comportamentale che di matrice tecnica, ricordiamo:

- possibile esposizione a contenuti violenti e non adatti alla loro età;
- videogiochi diseducativi;
- pubblicità ingannevoli;
- accesso ad informazioni scorrette;
- virus informatici in grado di infettare computer e cellulari;

- possibili contatti con adulti che vogliono conoscere e avvicinare bambini/e o ragazzi/e (adescamento);
- rischio di molestie o maltrattamenti da coetanei (cyber-bullismo);
- scambio di materiale a sfondo sessuale (sexting);
- uso eccessivo di Internet/cellulare (dipendenza).

Il nostro Istituto è impegnato in iniziative volte a promuovere la cultura dell'inclusione, del rispetto dell'altro/a e delle differenze, nonché l'utilizzo consapevole, positivo e responsabile delle Tecnologie dell'Informazione e della Comunicazione (TIC).

A tal fine è responsabilità di ciascun docente cogliere ogni opportunità per riflettere insieme agli alunni sui rischi in oggetto, nonché monitorare costantemente le relazioni interne alla classe, onde individuare possibili situazioni di disagio ed intervenire tempestivamente, anche mediante il ricorso a figure di sistema preposte (sportello d'ascolto), per sostenere il singolo nelle situazioni di difficoltà personale e indirizzare il gruppo verso l'instaurazione di un clima positivo, di reciproca accettazione e rispetto, nelle situazioni di difficoltà socio-relazionale.

Tale percorso interno è ulteriormente rinforzato dalla partecipazione a progetti e/o iniziative di formazione dei docenti, coerenti con i temi sopra menzionati, cui la scuola pone particolare attenzione. La scuola si avvale della collaborazione di enti e associazioni e polizia postale per realizzare incontri rivolti ad alunni, docenti e genitori con l'intento di fornire ogni elemento utile alla prevenzione e alla gestione dei problemi relativi alla sicurezza informatica

Rilevazione

La rilevazione dei casi è compito dell'intera comunità educante, secondo la sensibilità di ciascuno e la presenza in particolari momenti o contesti. A partire dalla corretta formazione e sensibilizzazione di tutti gli adulti coinvolti, docenti e personale ATA sono invitati a essere confidenti e custodi, diretti o indiretti, di ciò che le ragazze e i ragazzi vivono: si raccomanda di evitare ogni atteggiamento accusatorio o intimidatorio per riuscire a ricevere dai minori più fragili segnalazioni e confidenze circa situazioni problematiche vissute.

Le/gli insegnanti in particolare sono chiamati a essere anche torre di avvistamento, spazio di avamposto privilegiato delle problematiche, dei rischi, dei pericoli che bambine, bambini e adolescenti possono vivere e affrontare ogni giorno. Accorgersi tempestivamente di quanto accade e compiere azioni immediate di contrasto verso gli atti inopportuni -quando

non illegali- diviene fondamentale per poter evitare conseguenze a lungo termine che possano pregiudicare il benessere e una crescita armonica dei soggetti coinvolti.

Laddove il docente colga possibili situazioni di disagio connesse ad uno o più di uno tra i rischi elencati nel paragrafo “Prevenzione”, dovrà segnalare il caso e potrà chiedere il supporto del Consiglio di Classe, degli operatori dello sportello d’ascolto, delle FS Disagio e Nuove Tecnologie, del Dirigente Scolastico. Inoltre avrà cura di compilare la “scheda di segnalazione” sotto riportata.

Gestione dei casi

A seguito della segnalazione, verrà avviato un colloquio tra le componenti scolastiche sopra elencate, finalizzato a valutare la necessità di effettuare uno o più interventi di osservazione in classe e, successivamente, di pianificare adeguati interventi educativi e, ove necessario, di coinvolgere le famiglie per l'attivazione di un percorso comune e condiviso di sostegno al disagio. Le azioni poste in essere dalla scuola saranno dirette non solo a supportare le vittime, le famiglie e tutti coloro che sono stati spettatori attivi o passivi di quanto avvenuto, ma anche a realizzare interventi educativi rispetto a quanti abbiano messo in atto comportamenti lesivi, ove si tratti di soggetti interni all'Istituto. Nei casi di maggiore gravità si valuterà anche il coinvolgimento di attori esterni quali le forze dell'ordine e i servizi sociali.

RISCHI	AZIONI
Adescamento online (<i>grooming</i>)	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, <i>shopping</i> o <i>gambling</i> online, ...	Informazioni sul fatto che ciò può rappresentare una vera e propria patologia che compromette la salute e le relazioni sociali e che in taluni casi (per es. uso della carta di credito a

	insaputa di altri) rappresenta un vero e proprio illecito.
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 gli alunni: 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.
<i>Sexting</i> e pedopornografia.	Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale della navigazione. Verso gli alunni: 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.
--	--------------------------

Allegati:

SCHEDA DI SEGNALAZIONE		
ALUNNO		
CLASSE	SEZIONE	
PLESSO		
OSSERVAZIONE DIRETTA	EVENTO RIFERITO	DESCRIZIONE
☐	☐	Esposizione a contenuti violenti
☐	☐	Uso di videogiochi diseducativi
☐	☐	Accesso ed utilizzo di informazioni scorrette o pericolose
☐	☐	Scoperta ed utilizzo di virus in grado di infettare computer
☐	☐	Possibile adescamento
☐	☐	Cyberbullismo (rischio di molestie o maltrattamenti da coetanei)
☐	☐	Sexting (scambio di materiale a sfondo sessuale)
☐	☐	Dipendenza da uso eccessivo
Firma docente		

SCHEDA PER LA RILEVAZIONE DI VIOLAZIONE DELLE DISPOSIZIONI SULLA STRUMENTAZIONE PERSONALE

ALUNNO

CLASSE

SEZIONE

PLESSO

DOCENTE// COINVOLTO//

DATA DELLA VIOLAZIONE

DESCRIZIONE DEI FATTI

Firma docente/i coinvolto/i

Schema riepilogativo delle situazioni gestite legate a rischi online

Riepilogo casi

Scuola _____
Scolastico _____

Anno _____

N. °	Data	ora	Episodio (riassunto)	Azioni intraprese		Insegnante con cui l'alunno/a si è confidato	Firma
				Cosa?	Da chi?		