

E-policy POLITICA DI USO ACCETTABILE DELLE TECNOLOGIE DIGITALI ISTITUTO COMPRESIVO TRENTO 7 “RITA LEVI MONTALCINI”

Indice

1. Presentazione e premessa all'E-policy
 - 1.1. Scopo dell'E-policy e percorso di lavoro
 - 1.2. Importanza dell'E-policy
 - 1.3. Ruoli e responsabilità
 - 1.4. Condivisione e approvazione
 - 1.5. Tipologie di “culpa” e la gestione delle infrazioni
 - 1.6. Monitoraggio dell'efficacia della E-policy e suo aggiornamento
 - 1.7. Integrazione dell'E-policy con i Regolamenti esistenti

2. Formazione e curriculum
 - 2.1. Curriculum 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 e integrazione al Patto di corresponsabilità

3. Gestione dell'infrastruttura e della strumentazione TIC della e nella scuola
 - 3.1. Protezione dei dati personali
 - 3.2. Accesso ad Internet
 - 3.3. Account GSuite for Education
 - 3.4. Accertamento dei rischi e valutazione dei contenuti di internet
 - 3.5. Diritti di proprietà intellettuale
 - 3.6. Sanzioni per il mancato rispetto del Regolamento
 - 3.7. Gestione di Blog e/o Siti web
 - 3.8. Strategie organizzative della scuola per garantire la sicurezza
 - 3.9. Conclusioni

4. Rischi online: conoscere, prevenire e rilevare
 - 4.1. Sicurezza in Rete
 - 4.2. Cyberbullismo
 - 4.3. Hate speech
 - 4.4. Dipendenza da Internet e gioco online
 - 4.5. Sexting
 - 4.6. Adescamento online
 - 4.7. Pedo-pornografia

5. Segnalazione e gestione dei casi
 - 5.1. Cosa e come segnalare
 - 5.2. Pronto intervento sul Territorio

CAPITOLO 1. PRESENTAZIONE E PREMESSA ALL'E-POLICY

Nell'Istituto comprensivo Trento 7 "Rita Levi Montalcini" personale docente, non docente e studenti utilizzano le TIC (Tecnologie dell'Informazione e delle Comunicazioni).

Tutte le aule sono dotate di personal computer, nel plesso della scuola secondaria di primo grado ci sono anche le LIM.

L'Istituto offre agli insegnanti e agli alunni la fornitura di alcuni servizi Internet, cui si accede tramite pc negli spazi fisici sopraccitati, e fornisce ai docenti le relative credenziali di accesso:

- piattaforma di Istituto: Google Workspace
- registro di classe e registro personale del docente
- i genitori possono accedere al registro elettronico con l'utilizzo dello SPID

L'informatizzazione della scuola non si è limitata all'implementazione strumentale, ma è previsto anche un curriculum nel quale gli studenti imparino ad utilizzare le TIC per approfondire le conoscenze, recuperare documenti e scambiare informazioni.

Le "competenze digitali" sono fra le abilità chiave all'interno del Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente).

Si rende quindi necessario per l'Istituto Scolastico predisporre di una Policy, un documento programmatico finalizzato a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo. L'E-policy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.

L'E-policy è un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie digitali positivo, critico e consapevole, sia da parte degli studenti sia degli adulti coinvolti nel processo educativo.

Nell'E-policy si troveranno i termini "studente, alunno, allievo, bambino", utilizzati quali semplificazione di scrittura, con l'intento di non appesantire il testo inserendo le desinenze maschili e femminili. Nella pratica educativa, tuttavia, teniamo presente la necessità di considerare la persona nella sua specificità e peculiarità, anche di genere.

1.1 Scopo dell'E-policy e percorso di lavoro

Le TIC (Tecnologie dell'informazione e della comunicazione) rappresentano strumenti fondamentali nel processo educativo e per l'apprendimento degli studenti. Le "competenze digitali" sono fra le abilità chiave all'interno del Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente).

In un contesto sempre più complesso, diventa quindi essenziale dotarsi di una E-policy, un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie digitali positivo, critico e consapevole. L'E-policy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.

L'E-policy ha l'obiettivo, nello specifico, di esprimere la visione educativa e proposta formativa dell'Istituto, in riferimento alle tecnologie digitali. Nello specifico:

- l'approccio educativo alle tematiche connesse alle "competenze digitali", alla privacy, alla sicurezza online e all'uso delle tecnologie digitali nella didattica e nel percorso educativo;
- le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (TIC) in ambiente scolastico;
- le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
- le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

1.2 Importanza dell'E-policy

Attraverso l'E-policy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso di Internet.

L'E-policy fornisce, quindi, delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione ad un uso consapevole delle stesse.

1.3 Ruoli e responsabilità

Affinché l'E-policy sia davvero uno strumento operativo efficace per la scuola e tutta la comunità educante, è necessario che ognuno, secondo il proprio ruolo, s'impegni nella sua attuazione e promozione:

- a) **il dirigente scolastico** si attiva per garantire la sicurezza, anche on-line, di tutti i membri della comunità scolastica. Organizza, insieme al docente referente sulle tematiche del bullismo/cyberbullismo, corsi di formazione specifici per tutte le figure scolastiche sull'utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della comunicazione (TIC). Ha inoltre la responsabilità di gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.
- b) **l'Animatore digitale** supporta il personale docente in riferimento ai rischi online, alla protezione e gestione dei dati personali. È uno dei promotori di percorsi di formazione interna all'Istituto Comprensivo Trento 7 "Rita Levi Montalcini" negli ambiti di sviluppo della "scuola digitale" (con riferimento, ad esempio, allo sviluppo delle competenze digitali previste anche nell'ambito dell'educazione civica), in concorso con con la rete degli AD di Trento.
- c) **il Referente bullismo e cyberbullismo:** "Ogni Istituto scolastico, nell'ambito della propria autonomia, individua fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo" (Art. 4 Linee di orientamento per la prevenzione e il contrasto in ambito scolastico – Legge n.71/2017). Tale figura ha il compito di coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio. Fondamentale, dunque, il suo ruolo non solo in ambito scolastico ma anche in quello extrascolastico, in quanto (ove possibile) potrebbe coinvolgere con progetti e percorsi formativi ad hoc studenti, colleghi e genitori.
- d) **i Docenti** hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete, nell'integrare la propria attività didattica con l'uso delle tecnologie

digitali. I docenti accompagnano e supportano gli studenti nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete; segnalano al dirigente scolastico qualunque problema, violazione o abuso anche online che vedano coinvolti gli studenti.

- e) **Il personale Amministrativo, Tecnico e Ausiliario (ATA)** ciascuno per il proprio ruolo, svolge le mansioni assegnate in collaborazione con il dirigente scolastico e con il personale docente. È coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo.
- f) **gli Studenti** in relazione al proprio grado di maturità e consapevolezza, utilizzano al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti; con il supporto della scuola imparano a tutelare on line se stessi, i propri compagni e a rispettarli; partecipano attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e si fanno promotori di quanto appreso anche attraverso possibili percorsi di peer education;
- g) **i Genitori** in sinergia con l'Istituto Comprensivo Trento 7 "Rita Levi Montalcini", partecipano alle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali; si relazionano in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicano con loro nei casi di scarsa responsabilità nell'utilizzo delle tecnologie digitali o di Internet. È estremamente importante che accettino e condividano quanto scritto nel documento.
- h) **gli Enti educativi esterni e le associazioni** che entrano in relazione con la scuola si conformano alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC; promuovono comportamenti sicuri, la sicurezza on line e assicurano la protezione degli studenti durante le attività che si svolgono insieme.

1.4 Condivisione e approvazione

Il documento di E-policy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli studenti) si faccia a sua volta promotore del documento.

L'E-policy viene condivisa e approvata dal Collegio dei Docenti e dal Consiglio dell'Istituzione. Prima della sua approvazione e in fase di revisione, il documento viene condiviso con la Consulta dei Genitori che può proporre modifiche o integrazioni.

La comunicazione al personale, agli studenti, alla comunità scolastica avviene attraverso:

- la pubblicazione del documento sul sito istituzionale della scuola;
- la sottoscrizione all'inizio di ogni anno scolastico da parte delle famiglie del Patto di Corresponsabilità.

1.5 La "culpa" e la gestione delle infrazioni

Dato questo quadro, rispetto ad un profilo prettamente processuale anche in materia di bullismo e cyberbullismo (dunque non in via esclusiva), si può parlare di tre tipologie di "culpa":

- *culpa in vigilando*: concerne la mancata sorveglianza attiva da parte del docente responsabile verso il minore (così come da art. 2048 del c.c.). Tale condizione è superabile se ci si avvale di una prova liberatoria di non aver potuto impedire il fatto (recita il terzo comma dell'art. 2048 c.c.: "le persone indicate nei commi precedenti

sono liberate dalla responsabilità soltanto se provano di non aver potuto impedire il fatto”);

- *culpa in organizzando*: si riferisce ai provvedimenti previsti e presi dal dirigente scolastico ritenuti come non soddisfacenti e quindi elemento favorevole al verificarsi dell'eventuale incidente;
- *culpa in educando*: fa capo ai genitori, i quali hanno instaurato una relazione educativa con il figlio, ritenuta come non adeguata, insufficiente o comunque carente tale da metterlo nella situazione di poter recare danno a cose o persone terze.

La scuola gestirà le infrazioni all'E-policy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, anche valutando i diversi gradi di gravità di eventuali violazioni. La gestione delle infrazioni è responsabilità del dirigente scolastico, che attiva tutte le figure coinvolte, in particolare:

- il referente per la prevenzione e il contrasto del bullismo e del cyberbullismo;
- gli animatori digitali;
- i coordinatori e i consigli di classe.

Accertata l'infrazione, le figure designate comunicano con i docenti del Consiglio di classe e con i genitori.

Qualora l'infrazione richieda l'intervento della Polizia Postale o dell'autorità giudiziaria, si procederà alla comunicazione

1.6 Monitoraggio dell'efficacia della E-policy e suo aggiornamento

L' E-policy viene aggiornata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento saranno discusse con tutti i membri del personale docente. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone. Il dirigente o un docente da lui incaricato avrà il compito di revisionare e/o aggiornare l' E-policy.

1.7 L'integrazione dell'E-policy con i Regolamenti esistenti

Il regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con la normativa nazionale e provinciale.

CAPITOLO 2. FORMAZIONE E CURRICOLO

2.1 Curricolo sulle competenze digitali per gli studenti

I ragazzi usano la Rete quotidianamente, talvolta in modo più intuitivo e agile rispetto agli adulti, ma non per questo sono dotati di maggiori “competenze digitali”. Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la condivisione del curriculum digitale verticale, definendo gli obiettivi in termini di competenze, abilità e conoscenze.

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

È fondamentale che i docenti tutti siano formati e aggiornati sull'uso corretto, efficace ed efficiente delle TIC nella didattica al fine di usarle in modo integrativo ed inclusivo. Per questo la Scuola promuove corsi di formazione specifici anche in Rete con altri Istituti.

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

La scuola si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi online. Ciò avverrà tramite specifici momenti di aggiornamento che verranno organizzati dall'Istituto scolastico con la collaborazione sia del personale specializzato interno (Animatore digitale, referente bullismo e cyberbullismo) sia di personale esterno (professionisti qualificati) con il supporto della rete scolastica del territorio.

2.4 Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità. Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi continuativi e condivisi per accompagnare insieme ragazzi e bambini verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura.

La scuola garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali anche attraverso l'aggiornamento, oltre che del regolamento scolastico, anche del “Patto di corresponsabilità educativa”.

A tal fine la scuola si impegna a promuovere percorsi per genitori anche in Rete con altri Istituti o Enti del territorio.

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

La scuola promuove una comunicazione chiara ed esplicita con il personale, le famiglie e il territorio, in particolare attraverso:

- il sito istituzionale, costantemente aggiornato, che fornisce un'informazione puntuale e trasparente sulla documentazione e le attività della scuola;
- il registro elettronico, costantemente aggiornato dai docenti, mediante il quale le famiglie possono controllare assenze, voti, annotazioni e schede di valutazione; il registro elettronico consente anche una efficace comunicazione scuola-famiglia;
- la posta elettronica, canale preferenziale per la trasmissione di informazioni e comunicazioni tra tutti gli utenti.

La Scuola fornisce un supporto alle famiglie per le iscrizioni online ai diversi ordini di Scuola, mediante postazioni informatiche dedicate e personale applicato di segreteria.

3.1 Protezione dei dati personali

L'Istituto Comprensivo Trento 7 "Rita Levi Montalcini" opera a ogni livello rispettando tutte le normative vigenti in merito alla tutela della privacy, come indicato sul sito istituzionale. Nessuno è autorizzato a divulgare notizie private contenute nelle documentazioni elettroniche. Le password devono essere custodite in luoghi non accessibili a persone esterne o agli alunni della scuola. Ai genitori si chiederà ad inizio anno di firmare una liberatoria per la pubblicazione sul sito della scuola dei lavori dei propri figli e di eventuali foto in cui gli studenti non siano riconoscibili.

Essa è richiesta:

- a chi si iscrive per la prima volta nell'Istituto Comprensivo Trento 7 "Rita Levi Montalcini" o all'ordine successivo, attraverso la compilazione del modulo di iscrizione;
- a ciascun alunno all'inizio di ogni anno scolastico, attraverso l'apposita modulistica.

Sono permesse le riprese video e fotografiche di saggi e recite scolastiche se destinate a un ambito familiare o amicale e non alla diffusione. Va, quindi, prestata grande attenzione in quanto è proibita la pubblicazione delle medesime immagini su internet e in particolare sui social network.

Per far questo, resta necessario, infatti, il consenso informato delle persone presenti nel video e nelle fotografie. Per quanto riguarda la registrazione della lezione, essa è possibile esclusivamente per scopi personali, come ad esempio per motivi di studio individuale, previo avvertimento e consenso del docente interessato. Per una eventuale pubblicazione su Internet o sui social network, è necessario il consenso informato dei soggetti interessati, alunni e docenti presenti nella registrazione.

La scuola garantisce di non rendere accessibili informazioni che dovrebbero restare riservate o a non mantenere pubbliche, anche online, informazioni personali oltre il tempo necessario.

3.2 Accesso ad Internet

L'uso delle TIC rappresenta l'occasione per creare un nuovo ambiente di apprendimento in cui gli studenti possono trovare nuove opportunità per lavorare insieme, per studiare in modo creativo e autonomo, svolgere esercitazioni, ricercare informazioni, comunicare,

consolidare le nozioni apprese e diventare non solo fruitori ma anche autori di prodotti multimediali.

La rete internet e le connesse forme di comunicazione offrono occasioni di sviluppo espressivo di sé stessi e della propria identità, offrono canali e spazi in cui potersi relazionare con altre persone, anche fisicamente molto lontane, entrando in contatto con culture e paesi differenti. In questo modo l'apprendimento può diventare più semplice, più "fluidico" ed efficace. I ragazzi, se adeguatamente accompagnati e formati, possono trarre maggiori motivazioni all'apprendimento, attraverso un incremento della curiosità, sviluppando un senso critico nel discernere e nell'orientarsi all'interno della sconfinata quantità di informazioni presenti in rete.

Le nuove tecnologie si presentano come uno strumento efficace per la contestualizzazione degli argomenti, la realizzazione di esperienze significative di apprendimento, la riflessione e il consolidamento delle conoscenze acquisite e l'applicazione pratica e dinamica di quanto appreso. Non va inoltre dimenticato che la "competenza digitale" è inclusa tra le otto competenze chiave da assicurare nei percorsi formativi di tutti i cittadini europei secondo le raccomandazioni delle istituzioni comunitarie (Consiglio dell'Unione Europea e Parlamento Europeo 18 dicembre 2006 2006/962/CE). Le nuove tecnologie, inoltre, possono costituire un valido strumento di ausilio per gli studenti in situazione di svantaggio e/o con disturbi di apprendimento, elevando la soglia di attenzione e di interazione e permettendo un più proficuo recupero degli apprendimenti.

3.3 Account Google "Google Workspace"

Il nostro Istituto Comprensivo amplia le opportunità di utilizzo delle tecnologie digitali a scuola attraverso la piattaforma Google Workspace, che consente di comunicare e di gestire contenuti digitali con grande semplicità e flessibilità. La piattaforma garantisce sicurezza e privacy, connessione e interoperabilità, comunicazione facilitata tra docenti e studenti. Tutti gli studenti hanno accesso ai seguenti servizi:

- Comunicazione: Meet e Gmail (e-mail personale: nome.cognome@trento7.it)
- Programmazione: Calendar
- Archiviazione: Google Drive (Documenti, Fogli, Presentazioni, Moduli)
- Collaborazione: Google Classroom per la gestione di una classe virtuale.

I servizi principali di Google Workspace per gli studenti della nostra istituzione scolastica vengono forniti all'istituto scolastico in conformità all' "Accordo GSuite for Education" e alla "Modifica elaborazione dati GSuite for Education". I servizi vengono offerti esclusivamente per uso scolastico e didattico, pertanto la piattaforma fornita dal nostro Istituto è impostata in modo che l'account creato dalla scuola per ogni singolo alunno non possa essere usato al di fuori della stessa per scopi personali (ricevere/inviare/condividere materiale file, video ecc. proveniente da e verso l'esterno della piattaforma). L'obiettivo di questa iniziativa è fornire supporti, attraverso le tecnologie di rete, all'attività didattica e alla circolazione di informazioni esclusivamente interne.

Per ulteriori informazioni sulla configurazione della piattaforma e sui termini del servizio si possono visitare le seguenti pagine web:

- Informazioni sulla privacy e la sicurezza di Google Suite for Education: <https://support.google.com/a/answer/60762?hl=it>
- Termini di servizio: <https://www.google.com/policies/terms/>
- Norme sulla privacy: <https://www.google.com/policies/privacy/>

Ai fini del rispetto del Regolamento Europeo UE/2016/679 in materia di protezione dati personale, l'Istituto Comprensivo Trento 7 "Rita Levi Montalcini" fornisce agli utenti apposita informativa.

3.4 Accertamento dei rischi e valutazione dei contenuti di internet

La scuola si fa carico di tutte le precauzioni possibili per garantire agli studenti l'accesso a materiale appropriato. Gli studenti imparano ad utilizzare i mezzi di ricerca su Internet, che includono i cataloghi per soggetto e l'uso dei motori di ricerca. Le abilità di gestione delle informazioni comprendono:

- la garanzia di validità, la diffusione e l'origine delle informazioni a cui si accede;
- la ricerca del nome dell'autore, dell'ultimo aggiornamento del materiale e dei possibili altri link al sito;
- il rispetto dei diritti d'autore e dei diritti di proprietà intellettuale (netiquette, galateo di internet, Creative Commons);
- gli studenti devono essere pienamente coscienti dei rischi a cui si espongono quando sono in rete.

Il docente che organizza l'attività didattica supportata dalle TIC rappresenta la migliore forma di prevenzione dai rischi dell'uso improprio della rete da parte degli studenti. Ogni docente deve:

- illustrare ai propri alunni le regole di utilizzo dei dispositivi informatici con particolare riferimento all'uso di Internet;
- discutere con i propri alunni della netiquette (cioè regole comuni di accesso e utilizzo di chat, forum, mail e di qualsiasi altro tipo di comunicazione sincrona e asincrona);
- informare, anziché censurare, gli alunni al fine di renderli coscienti dei rischi in cui possono incorrere ed a riconoscere gli aspetti negativi di Internet come la pornografia, la violenza, il razzismo e lo sfruttamento dei minori;
- responsabilizzare gli alunni ad un utilizzo consapevole dei servizi e dei contenuti della rete per conoscerne gli effetti cognitivi, affettivi e comportamentali, oltre ad una conoscenza tecnica utile a gestire correttamente gli strumenti tecnologici e a monitorare la navigazione affinché gli alunni non accedano a siti non appropriati.

Gli Studenti sono tenuti a:

- utilizzare le TIC assegnate loro per lo svolgimento delle attività autorizzate, sempre sotto la supervisione del docente per le attività che si svolgono nell'Istituto Comprensivo Trento 7 "Rita Levi Montalcini". Nelle situazioni particolari individuate e riconosciute dal Consiglio di Classe è possibile l'utilizzo degli strumenti tecnologici personali degli alunni;
- utilizzare penne USB protette da password e da antivirus, CD-ROM e DVD o altri dispositivi esterni anche personali, ma collegati alla rete della scuola o ad una rete comunque controllata dall'insegnante, previa autorizzazione del docente responsabile dell'attività in essere;
- accedere alla rete solo in presenza dell'insegnante responsabile dell'attività o previa autorizzazione;
- accedere all'ambiente di lavoro con l'account fornito dalla scuola, archiviare i propri documenti secondo le indicazioni fornite dai docenti e chiudere correttamente la propria sessione di lavoro;
- in caso di riscontro di malfunzionamenti della strumentazione e/o di contatto accidentale con contenuti non adeguati al contesto, rivolgersi all'insegnante.

Agli studenti è vietato:

- usare Internet per scopi diversi da quelli didattici;
- usare dispositivi di registrazione audio, videocamere o fotocamere per registrare video o fare foto in classe senza il permesso dell'insegnante e senza il consenso della persona che viene registrata o ripresa;
- scaricare musica, video e programmi da Internet o qualsiasi file senza il consenso dell'insegnante;
- utilizzare i social network;
- giocare sul computer, in rete o offline (a meno che il gioco non faccia parte di una lezione e sia supervisionato dall'insegnante);
- usare i dispositivi al di fuori dall'orario di lezione come ad esempio pause, ricreazione, uscite didattiche, visite guidate, viaggi d'istruzione, attività facoltative extracurricolari, manifestazioni sportive, spettacoli teatrali ecc., se non con l'esplicita autorizzazione del docente responsabile della classe.
- utilizzare la Rete per deridere, offendere, denigrare compagni, docenti, personale scolastico, parenti/amici dei compagni sia in orario scolastico sia in orario extrascolastico; si ricorda che il cyberbullismo è un reato e qualsiasi atto degli studenti che dovesse configurarsi come reato verrà denunciato d'ufficio alle forze dell'ordine. Alla denuncia d'ufficio può sommarsi la querela da parte della persona chiamata in causa.

3.5 Diritti di proprietà intellettuale

Gli studenti devono rispettare e proteggere la proprietà intellettuale altrui:

- non è ammessa la copia o il plagio di testi, immagini, filmati...;
- non è ammessa la violazione dei copyright: si deve sempre attribuire, citare e richiedere il permesso degli autori o creatori delle informazioni o dei media originali (se richiesto dalla legge o da accordo) prima di utilizzare qualsiasi materiale.

3.6 Sanzioni per il mancato rispetto del Regolamento

L'uso della tecnologia, sia essa di proprietà della scuola sia esso un dispositivo personale degli studenti, comporta responsabilità personali. Ci si aspetta che gli studenti rispettino le regole e che agiscano con correttezza e senso di responsabilità. Il mancato rispetto di questi termini e condizioni potrà comportare, a seconda della gravità dell'infrazione, la temporanea o la permanente perdita di accesso alla rete nonché altre azioni disciplinari previste dal Regolamento interno dell'Istituto e legali, se necessario.

Gli studenti sono ritenuti responsabili delle loro azioni e sono incoraggiati a segnalare immediatamente ogni uso scorretto, anche ad opera dei compagni, al loro insegnante.

3.7 Gestione di blog e/o siti web

Le pagine di blog e/o siti web sono gestite dall'insegnante responsabile ed è sua cura garantire che il contenuto sia appropriato. Potranno essere pubblicati i materiali prodotti dagli studenti solo dopo aver chiesto il permesso scritto ai loro genitori. Nelle fotografie e nei video potranno essere presenti studenti in foto di gruppo, ma con una definizione sufficientemente bassa da non permettere una successiva elaborazione elettronica o il riconoscimento certo. Non saranno ammesse fotografie che riprendono gli studenti a mezzobusto o autoritratti.

3.8 Strategie organizzative della scuola per garantire la sicurezza

Gli alunni possono accedere all'uso dei computer solo se accompagnati dai docenti. Il sistema informatico delle aule di informatica della scuola ed i computer presenti nelle aule vengono regolarmente controllati dai responsabili dei laboratori e dai docenti per monitorare il corretto funzionamento dell'hardware e/o del software, segnalando le eventuali disfunzioni all'assistenza tecnica.

La scuola controlla, tramite il personale tecnico, i file utilizzati ed i siti visitati in ogni computer in dotazione. I software utilizzati devono essere quelli autorizzati dalla scuola e/o liberi da licenza. Il sistema informatico della scuola è provvisto di firewall e di software antivirus con aggiornamento automatico per proteggere i computer della rete da accessi esterni.

3.9 Conclusioni

Si ribadisce che gli utenti sono resi responsabili nel loro uso di Internet e sono consapevoli che:

- l'Istituto Comprensivo Trento 7 "Rita Levi Montalcini" non può garantire l'accuratezza e l'affidabilità delle informazioni reperite in rete e non può assumersi alcuna responsabilità né tantomeno supervisionare i contenuti a cui un utente accede (anche inavvertitamente);
- l'Istituto Comprensivo Trento 7 "Rita Levi Montalcini" non si assume alcuna responsabilità per danni, perdite, costi o spese derivanti direttamente o indirettamente dall'uso dei servizi informatici e di consultazione Internet;
- i minori possono avvalersi dei servizi informatici all'interno dell'Istituto Comprensivo Trento 7 "Rita Levi Montalcini" a condizione che siano supervisionati o guidati da un insegnante o altro adulto responsabile;
- nel rispetto della normativa vigente sulla sicurezza in rete, gli utenti devono usare ogni accortezza per evitare di danneggiare apparecchi informatici o software, non devono alterare la configurazione di software e di sistema, non devono usare le postazioni di lavoro nell'Istituto Comprensivo Trento 7 "Rita Levi Montalcini" a fini illegali o immorali.

Le informazioni sulla PUA della scuola avvengono nelle seguenti modalità:

Per gli studenti: gli studenti ricevono istruzioni dai docenti per un utilizzo responsabile di internet, del laboratorio di informatica e delle risorse a disposizione per le attività didattiche;

Per i genitori: il documento viene inviato a tutte le famiglie per la condivisione; ai genitori, inoltre, viene richiesta l'autorizzazione per la pubblicazione dei lavori dei propri figli, delle fotografie e video sul sito della scuola, per l'accesso ad eventuali piattaforme di classe e ambienti di condivisione con account fornito dall'istituto Comprensivo Trento 7 "Rita Levi Montalcini".

CAPITOLO 4. RISCHI ONLINE: CONOSCERE, PREVENIRE E RILEVARE.

4.1 Sicurezza in Rete

L'Istituto Comprensivo Trento 7 "Rita Levi Montalcini" si prefigge come obiettivo quello di fornire a tutta l'utenza le competenze necessarie al fine di tenere comportamenti responsabili e corretti nella fruizione delle TIC e della rete, così da poter prevenire i rischi in cui ci si può imbattere.

Per quanto riguarda l'uso delle TIC, il personale in servizio presso la Scuola, gli alunni e le loro famiglie sono informati e formati in merito alle modalità di un utilizzo sicuro, negli ambienti scolastici o all'esterno, dei diversi device, quali tablet, pc, smartphone, fornendo loro indicazioni su come gestire impostazioni di cronologia, cookie, cache, firewall, malware e virus in genere.

Fondamentale è anche diffondere le nozioni per una navigazione sicura, corretta e responsabile in merito a:

- uso di siti e piattaforme istituzionali, compresi il sito della scuola, il registro online e le piattaforme usate durante le attività didattiche;
- gestione degli account, con attenzione alla conservazione delle credenziali di accesso;
- misure di sicurezza per la fornitura dei dati personali, ponendo attenzione alle situazioni in cui ciò è sconsigliato o poco opportuno;
- gestione e netiquette delle caselle di posta elettronica in genere e delle mailing list, anche per ciò che riguarda la possibilità di imbattersi in comunicazioni fraudolente, regole per l'upload e il download in sicurezza di qualsiasi tipo di file;
- gestione delle relazioni sui social network, nelle chat e nelle applicazioni di instant messaging, soprattutto a proposito della condivisione e pubblicazione di foto, video, informazioni personali, conversazioni;
- rischi di entrare in siti non opportuni, pornografici, di reclutamento a fini illegali, fraudolenti;
- normativa vigente sulla privacy e sulle procedure di dematerializzazione messe in atto dalla Scuola;
- rischi più diffusi in rete, anche a causa di un utilizzo non responsabile della stessa, in particolare cyberbullismo, sexting, grooming.

4.2 Cyberbullismo: cos'è e come prevenirlo

Il cyberbullismo è la manifestazione in Rete di un fenomeno più ampio e meglio conosciuto come bullismo. Quest'ultimo è caratterizzato da azioni violente e intimidatorie esercitate da un bullo, o un gruppo di bulli, su una vittima. Le azioni possono riguardare molestie verbali, aggressioni fisiche, persecuzioni, generalmente attuate in ambiente scolastico. Oggi la tecnologia consente ai bulli di infiltrarsi nelle case delle vittime, di materializzarsi in ogni momento della loro vita, perseguitandole con messaggi, immagini, video offensivi inviati tramite smartphone o pubblicati sui siti web tramite Internet. Il bullismo diventa quindi cyberbullismo. Il cyberbullismo definisce un insieme di azioni aggressive e intenzionali, di una singola persona o di un gruppo, realizzate mediante strumenti elettronici (sms, mms, foto, video, email, chat rooms, instant messaging, siti web, telefonate), il cui obiettivo è quello di provocare danni ad un coetaneo incapace di difendersi.

Possiamo parlare di cyberbullismo se l'atto è:

- **intenzionale**: il comportamento denigratorio messo in atto deve essere volontario e non accidentale;

- **ripetuto**: il cyberbullismo riflette un vero e proprio modello di comportamento, non solo un incidente isolato, e ciò è uno dei motivi per cui esso può diventare emotivamente e psicologicamente molto dannoso per la vittima; la stessa natura del cyberbullismo e il fenomeno della viralità in rete rende molto probabile la ripetitività del danno alla vittima;
- **dannoso**: la vittima deve percepire il danno psicologico e morale che le viene inflitto;
- **messo in pratica attraverso computer, cellulari e dispositivi elettronici**: l'uso delle tecnologie digitali è il primo elemento distintivo fra bullismo e cyberbullismo

Per i casi di bullismo o cyberbullismo, la scuola si prodiga nella tutela dei minori coinvolti, senza renderli in alcun modo identificabili, con dati o altri strumenti.

4.3 Hate Speech

“L’incitamento all’odio deve essere inteso come comprensivo di tutte le forme di espressione che diffondono, incitano, promuovono, o giustificano l’odio razziale, la xenofobia, l’antisemitismo o altre forme d’odio generate dall’intolleranza, ivi comprese: l’intolleranza espressa dal nazionalismo, e dall’etnocentrismo aggressivi, la discriminazione e l’ostilità nei confronti delle minoranze, dei migranti, e delle persone con origine straniera”. (<http://www.coe.int/it/web/freedom-expression>).

Il fenomeno dell’hate speech è complesso: i giovani rischiano di essere maggiormente esposti sia per il massiccio uso dei social sia per la scarsità (o la mancanza) di situazioni in cui prendere consapevolezza del discorso d’odio. La scuola si trova in prima linea di fronte al difficile compito di affrontare questo fenomeno, che ha senza dubbio forti ripercussioni nelle relazioni tra i pari e nella propria relazione col mondo.

Anche in questo caso si rende necessario affrontare l’hate speech con i propri studenti attraverso l’educazione ai media, l’educazione interculturale e il coinvolgimento attivo dei ragazzi e delle ragazze (Fonte: Bricks against the hate speech)

4.4 Dipendenza da Internet e gioco online

La Dipendenza da Internet fa riferimento all’utilizzo eccessivo ed incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o essere associato ad isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e “craving” (irrefrenabile voglia di utilizzo della Rete).

Di seguito alcuni aspetti utili per fare una prima valutazione di rischio rispetto ad un utilizzo disfunzionale/patologico della Rete:

- uso eccessivo
- spesso associato ad una perdita del senso del tempo che passa o la dimenticanza di bisogni primari (come ad esempio mangiare e dormire);
- senso di straniamento – con la manifestazione di sentimenti di rabbia, tensione e/o depressione quando il computer o la Rete sono inaccessibili;
- tolleranza – con il bisogno di accessori sempre migliori per il computer o di un sempre maggiore tempo di utilizzo;
- ripercussioni negative – incluse discussioni, bugie (soprattutto riguardo al tempo passato online), isolamento sociale e scarsi risultati in ambito scolastico.

Anche i videogiochi sono come una risposta ai bisogni di bambini e adolescenti inseriti in contesti eterogenei ed interattivi caratterizzati dall’uso coinvolgente e diffuso delle nuove tecnologie. In tal senso, gli aspetti positivi legati ai videogiochi si riferiscono al fatto che gli stessi possono:

- contribuire allo sviluppo di abilità tecniche e strategiche;
- migliorare la coordinazione oculo-motoria;
- contribuire all'acquisizione di abilità di problem solving.

Al tempo stesso le criticità connesse all'utilizzo dei videogiochi possono essere:

- la dipendenza legata ad un loro uso eccessivo, con il rischio di trascurare lo studio e le relazioni amicali;
- se utilizzati per molte ore, possibili problemi di salute legati all'eccessivo stress, a disturbi del sonno, manifestazioni di ansia ecc., ma anche il rischio di sviluppare una miopia indotta dall'eccessivo sforzo di messa a fuoco ravvicinata (questo vale in generale anche per il cellulare);
- i rischi di subire violazioni della privacy;
- contatti indesiderati nei casi di videogiochi online;
- esposizione a contenuti potenzialmente dannosi;
- rischio di virus e malware sui dispositivi (a causa di app infette) e di phishing;
- rischi specifici legati al gioco d'azzardo online, inclusa la ludopatia.

Il gioco d'azzardo online, che è cosa diversa dal videogioco, in molti casi sfugge alle restrizioni di età vigenti nel nostro paese, stabilite proprio per la protezione dei minori. Ad esempio, la registrazione sulle piattaforme di gioco e di scommessa può essere fatta con documenti di identità del genitore o di un amico maggiorenne: vi sono anche siti di gioco illegale che, in quanto tali, non si preoccupano di applicare barriere di ingresso ai minori.

Il minore è più vulnerabile dell'adulto alle sollecitazioni emotive ed alla ricerca di gratificazione legate alla scommessa e alla vincita, risultando dunque più esposto al rischio di dipendenza patologica e gioco compulsivo. Ancora, ci sono chat di gioco (ambienti assolutamente non controllati e non controllabili) che espongono al rischio di essere attratti in chat di appuntamenti, che offrono scommesse illegali, giochi a tema erotico ecc., che puntano proprio ai soggetti vulnerabili ed ai minori.

I genitori, oltre ad educare con scrupolo i figli su queste problematiche, dovrebbero osservare attentamente i loro comportamenti, dal tempo trascorso a giocare online, alle modalità di gioco e di relazione con altri giocatori, all'uso del denaro di cui i ragazzi dispongono o all'uso eventualmente non autorizzato della carta di credito dei genitori. Quando si acquista un videogioco, occorre prestare attenzione alla classificazione PEGI ed ai descrittori di contenuto presenti; quando si acconsente alla partecipazione dei figli ad una Community di Gioco, bisogna innanzitutto documentarsi sulle sue funzionalità e valutare personalmente i potenziali rischi che esse presentano; poi illustrare ai ragazzi i pericoli individuati ed istruirli sulle opportune precauzioni. È sconsigliabile, infine, far utilizzare ai figli la propria carta di credito per acquisti online anche preventivamente approvati, per evitare che ne possano fare successivamente uso senza chiedere il consenso: meglio una carta prepagata con piccole somme e con estratto conto consultabile dal genitore.

4.5 Sexting

Il sexting, crasi dei termini "sex" (sesso) e "texting" (pubblicare testo), è l'invio e/o la ricezione e/o la condivisione di video o immagini sessualmente espliciti (via smartphone o tramite Internet e i social network, ivi compreso WhatsApp), che ritraggono di se stessi ritratti nudi o seminudi (Levick & Moon 2010).

Esso può essere altresì descritto come “lo scambio di messaggi o immagini a sfondo sessuale” (Livingstone et al., 2011) e il “creare, condividere, inoltrare immagini di nudo o seminudo attraverso telefoni cellulari e/o internet” (Lenhart, 2009).

Molti sono i rischi legati al sexting: non si può tornare indietro facilmente in quanto l'immagine o il video possono essere già stati scaricati e inviati ad altri; si rischia di avere problemi in futuro nel senso che le immagini spinte potrebbero, a distanza di anni, riapparire causando problemi alla reputazione sia personale che professionale; si corre il pericolo di diventare una vittima di cyberbullismo o di essere adescata/o on line o essere ricattato.

L'impatto che tali esperienze possono avere sulla vittima di sexting possono essere, quindi, molto dolorose ed estreme perché impattano sulla sua identità personale e sociale e sulla sua credibilità fra i pari, molto importante soprattutto in preadolescenza e in adolescenza. Tra le conseguenze: perdita di fiducia in sé stessi e negli altri; perdita di autostima; tristezza, ansia e depressione; autolesionismo; disturbi alimentari ed in casi più estremi, il suicidio.

4.6 Adescamento online

L'adescamento o grooming (dall'inglese “groom”=curare, prendersi cura) è una tecnica di manipolazione psicologica messa in atto da un adulto nei confronti di un bambino o un adolescente con l'obiettivo di instaurare con il minore una relazione intima e/o sessualizzata. L'adulto potenzialmente abusante induce il minore a superare le sue resistenze emotive conquistandone pian piano la fiducia. Per conquistarsi la fiducia del minore l'adescatore si presenta ai suoi occhi paziente, affettuoso, comprensivo. Spesso l'adulto abusante sfrutta proprio alcuni bisogni essenziali del bambino o dell'adolescente, come quello di essere compreso, di ricevere attenzioni esclusive, di sentirsi riconosciuto e apprezzato nell'immagine e come persona. L'adescatore fa così leva anche sulle insicurezze e le fragilità che sovente caratterizzano i bambini e gli adolescenti, mostrandosi comprensivo e sempre disponibile all'ascolto. Talvolta, poi, l'adulto abusante può anche camuffare la propria reale identità, presentandosi come un'altra persona. Il percorso di adescamento è graduale e si sviluppa per step e può durare diversi mesi, il tempo necessario affinché il minore si fidi e si affidi completamente.

4.7 Pedo-pornografia

Per "pornografia infantile" si intende ogni tipo di materiale che rappresenti visivamente un bambino in atteggiamenti sessualmente espliciti, reali o simulati. Ma anche qualsiasi rappresentazione degli organi sessuali di un bambino per scopi sessuali.

La pedopornografia online è un reato specifico (art. 600-ter comma 3 del c.p.) che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video che ritraggono persone minorenni coinvolte in comportamenti sessualmente espliciti, concrete o simulate o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.

In Italia, il 2 marzo 2006 è entrata in vigore la Legge n. 38/06 “Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet” che introduce delle modifiche alle disposizioni già contemplate dalla Legge 3 agosto 1998, n.269 "Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù".

CAPITOLO 5. SEGNALAZIONE E GESTIONE DI CASI

L'attivazione di percorsi di digital literacy (alfabetizzazione digitale) rivolti a giovani, educatori, insegnanti e genitori, con una particolare attenzione allo sviluppo di quelle "competenze digitali" in grado di promuovere fra i ragazzi un uso consapevole e responsabile delle nuove tecnologie rappresenta, senza dubbio, la risposta migliore al problema del cyberbullismo e di un uso distorto e patologico della rete da parte dei minori.

Tutte le componenti della scuola, in particolare personale docente e genitori, devono essere costantemente formate, informate e aggiornate in particolare sui fenomeni del bullismo e del cyberbullismo.

5.1 Cosa e come segnalare

L'Istituto Comprensivo Trento 7 "Rita Levi Montalcini" si impegna a formare e aggiornare i docenti sulle modalità e gli indicatori per riconoscere eventuali casi o situazioni a rischio e sulle procedure da seguire. Chiunque entri in possesso di dati certi deve avere la possibilità di denunciarli in forma tutelata: colui che denuncia non deve correre rischi e deve avere tutte le possibili tutele.

Nel momento in cui si è a conoscenza di situazioni di bullismo o cyberbullismo o di uso distorto della rete:

- il docente avvisa immediatamente il dirigente scolastico;
- il docente stende un verbale dell'episodio, nel quale vengono riportate le situazioni problematiche rilevate;
- il dirigente scolastico convoca la famiglia per informarla dell'accaduto;
- il docente svolge un colloquio approfondito, in separata sede, con la vittima e con il bullo o cyberbullo, per acquisire informazioni aggiuntive, che è tenuto a verbalizzare;
- a seconda dei casi, si informano i servizi sociali e/o la Polizia Postale;
- in caso di eventi particolarmente gravi o con profili che si possono presumere penali, è obbligatorio ricorrere all'autorità giudiziaria;
- gli studenti protagonisti di atti di bullismo o cyberbullismo devono essere guidati a comprendere la gravità degli atti compiuti; devono essere sanzionati come da regolamento e, contestualmente, devono essere obbligati a comportamenti attivi di natura risarcitoria e riparatoria, volti al perseguimento di una finalità educativa;
- a livello formativo, i docenti tengono conto dell'accaduto nel corso del processo didattico;
- viene fatta salva la possibilità di ciascuno studente o genitore di segnalare al dirigente oppure mediante la mail dedicata l'episodio, anche in forma anonima.

5.2 Pronto intervento sul Territorio

In caso di necessità ci si può rivolgere ai seguenti servizi gestiti da Telefono Azzurro (<http://www.azzurro.it/it/sostegno>), come suggerito dalla Helpline di Generazioni Connesse (<https://www.generazioniconnesse.it/>):

- Linea di ascolto 1.96.96, attiva 24 ore su 24, 365 giorni all'anno;
- Chat, attiva dalle 8.00 alle 22.00 in settimana, dalle 8.00 alle 20.00 il sabato e la domenica.

Tali canali accolgono qualsiasi richiesta d'ascolto e di aiuto da parte di bambini e ragazzi fino ai 18 anni, o da parte di adulti che si vogliono confrontare su situazioni di disagio/pericolo che vedono coinvolti dei minori come:

- uso sicuro di Internet e dei social network
- adescamento online/grooming

- pedopornografia
- cyberbullismo
- sexting, pornografia e sessualità online degli adolescenti
- gioco d'azzardo online
- violazione della Privacy
- furto di identità in rete
- esposizione a contenuti nocivi online
- dipendenza da Internet
- esposizione a siti violenti, razzisti, che invitano al suicidio o a comportamenti alimentari scorretti (pro-anoressia e pro-bulimia)
- dipendenza da shopping online
- videogiochi online non adatti ai ragazzi.

Per quanto riguarda la Provincia Autonoma di Trento si fornisce lo schema generale di procedura impostata secondo le seguenti fasi:

- A. ascolto, accoglienza e definizione del caso
- B. situazioni di pregiudizio (esclusi i reati procedibili d'ufficio)
- C. reati procedibili d'Ufficio.

In caso di necessità di un parere legale:

Riferimento Provinciale (Garante dei diritti dei minori P.A.T)

tel. 0461 213201 numero verde: 800 85 1026

Email: difensore.civico@pec.consiglio.provincia.tn.it

Approvato dal Collegio dei docenti in data 20/12/2022

Approvato dal Consiglio dell'Istituzione in data 22/12/2022 con delibera n. 18