ISTITUTO COMPRENSIVO
di TIONE

E- POLICY
di uso accettabile

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 dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo.

1. **Presentazione e premessa all'*E-policy***
   - 1.1. Scopo dell'*E-policy* e percorso di lavoro
   - 1.2. Ruoli e Condivisione
   - 1.3. Responsabilità
   - 1.4. Integrazione della Policy con Regolamenti esistenti
   - 1.5. Monitoraggio dell'implementazione della E-policy e suo aggiornamento
2. **Formazione e curricolo**
   - 2.1. Curricolo sulle competenze digitali per gli studenti
     - 2.1.1. Peer education tra alunni
   - 2.2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) 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. Autenticazione e risorse
   - 3.3. Server
   - 3.4. Client
   - 3.5. Dispositivi di sicurezza
   - 3.6. Rete cablata e WiFi
   - 3.7. Posta e sistemi collaborativi
   - 3.8. Sito Web istituzionale
   - 3.9. Piattaforma AVAC (Area Virtuale di Apprendimento Cooperativo)
   - 3.10. Registro elettronico
   - 3.11. Strumentazione personale
     - 3.11.1. Studenti
     - 3.11.2. Docenti
     - 3.11.3. Personale della scuola
4. **Rischi on line: conoscere, prevenire e rilevare**
   - 4.1. Sensibilizzazione e prevenzione
   - 4.2. Cyberbullismo: che cos'è e come prevenirlo
   - 4.3. Hate speech: che cos'è e come prevenirlo
   - 4.4. Dipendenza da Internet e gioco online
   - 4.5. Sexting
   - 4.6. Adescamento online
5. **Segnalazione e gestione dei casi**
6. **Allegati**
   - 6.1. Revisione e modifiche della E-Policy
   - 6.2. Monitoraggio, segnalazioni e sanzioni
   - 6.3. Scheda di segnalazione
   - 6.4. Patto di corresponsabilità

1. Presentazione e premessa all'*E-policy*

1.1. Scopo dell'*E-policy* e percorso di lavoro

Il nostro Istituto avverte come esigenza, per camminare al passo con i tempi, quella di incrementare l'uso delle tecnologie informatiche nella didattica e nell'organizzazione generale della scuola affinché Internet, inestimabile risorsa per l'educazione e l'informazione, venga utilizzato per fornire nuove opportunità nel fare ricerca, comunicare, documentare il proprio lavoro, pubblicare elaborati e mettere in comune esperienze. La scuola utilizza il proprio sito istituzionale, il registro elettronico ISI-REL e la piattaforma AVAC, a cui possono accedere, a seconda dello scopo (amministrativo, informativo, didattico), i diversi attori dell'Istituto.

Allo stesso tempo, però, l'uso sempre più esteso di piattaforme in rete e dispositivi portatili ha esposto gli utenti, e in particolare i minori, i soggetti con divario digitale o con limitate competenze informatiche, a nuovi rischi, tanto più rilevanti quanto meno è diffusa una cultura relativa ai modi legittimi di usare la rete e alla consapevolezza delle funzioni rese possibili.

È in questo quadro che la nostra Scuola ha deciso di sviluppare e attuare il progetto "Generazioni Connesse" (www.generazioniconnesse.it) attraverso la realizzazione di diversi interventi tra cui l'elaborazione di una E-Safety Policy d'Istituto, cioè di un proprio codice di condotta nella prevenzione e gestione dei casi di (Cyber)bullismo e di un regolamento di sicurezza informatica. Questo nuovo documento intende dare nel nostro Istituto un impulso allo sviluppo di un uso corretto e consapevole di Internet, sia tramite il richiamo a norme vigenti, sia con l'indicazione di prassi opportune per un uso sempre più professionale da parte di tutto il personale e per la prevenzione dei rischi e la gestione delle emergenze.

1.2. Ruoli e Condivisione

La E-policy d'Istituto si applica a tutti i membri della scuola, compreso il personale, gli studenti, i genitori, gli utenti della comunità che ne hanno accesso. La sua condivisione segue il seguente iter:

- è stesa dalle insegnanti referenti individuate: Cornelia Dallatorre e Milena Valenti per la Scuola primaria, Isabella Antolini e Maria Grazia Pedretti per la Scuola Secondaria di primo grado (mentre era in servizio presso il nostro istituto ha collaborato anche la prof.ssa Michela Alimonta);
- è letta e condivisa dal Dirigente Scolastico, prof. Alberto Paris;
- è approvata dal Collegio dei Docenti;
- è approvata dal Consiglio dell'Istituzione;
- è pubblicata sul sito della scuola;

- è discussa con gli studenti e i genitori, all'inizio del primo anno, tramite il *Patto di Corresponsabilità*, che sarà sottoscritto dalle famiglie e rilasciato alle stesse;
- è condivisa e accettata dal personale scolastico;
- sarà rinnovata periodicamente attraverso osservazioni rilevate *in itinere* e per adattarsi alle innovazioni che si presenteranno.

1.3. Responsabilità

La gestione delle infrazioni è responsabilità del Dirigente Scolastico, prof. Alberto Paris, che attiva tutte le figure coinvolte, quali:

- responsabile della sicurezza online, Isabella Antolini [1]
- animatore digitale, Cornelia Dallatorre.

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 si procederà come da protocollo.

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.

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/la figlio/a, ritenuta come non adeguata, insufficiente o comunque carente tale da metterlo/a nella situazione di poter recare danno a terzi.

1.4. Integrazione della Policy con Regolamenti esistenti

[1] Art. 4 *Linee di orientamento per la prevenzione e il contrasto in ambito scolastico* – Legge n.71/2017: "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").

La presente E-policy viene integrata al Piano di Istituto e alla Carta dei Servizi, entrambi visionabili sul sito della scuola (http://www.ictione.tn.it). Tali documenti manifestano l'obiettivo comune di potenziare l'apprendimento mediato dalle tecnologie digitali e nel medesimo tempo condividono l'interesse a promuovere azioni che assicurino una giusta sicurezza nel suddetto ambito.

1.5. Monitoraggio dell'implementazione della E-policy e suo aggiornamento

La E-policy sarà riesaminata annualmente o quando si verificheranno cambiamenti significativi per quanto riguarda le tecnologie in uso all'interno della scuola e ogni modifica della Policy sarà discussa con tutti i membri del personale docente. Le revisioni saranno memorizzate per eventuali controlli, sulla base dell' Allegato 1.

Nell'ambito del monitoraggio dell'implementazione della E-Safety Policy si terranno in considerazione i dati annuali sulla base dell'Allegato 2.

2. Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

Oggi la scuola è immersa in un paesaggio educativo assai più ricco di stimoli rispetto al passato e l'apprendimento scolastico non è che uno dei tanti canali per l'acquisizione di abilità e competenze.

In questo ultimo decennio la diffusione delle tecnologie massmediali si è fatta sempre più capillare e pervasiva, cosicché la scuola non detiene più un sicuro monopolio delle informazioni e delle vie di apprendimento. Queste circostanze la chiamano, come non mai, ad assumere un ruolo di "guida": è sua inderogabile responsabilità condurre gli alunni ad acquisire e consolidare le conoscenze e le competenze di base indispensabili per la conquista di un metodo di apprendimento autonomo e valido per l'intero arco della vita. (Imparare ad imparare)

In questo scenario le tecnologie digitali stanno esercitando un impatto importante sulla formazione, sull'istruzione e sull'apprendimento, mediante lo sviluppo di ambienti più flessibili, adatti a favorire l'inclusione, a sviluppare le abilità del problem solving, il pensiero critico, la creatività e la capacità di cooperare.

In quest'ottica, negli ultimi anni, abbiamo assistito ad importanti interventi ministeriali di spinta all'innovazione didattica e alla digitalizzazione delle Istituzioni.

Il documento che più di tutti illustra e specifica i parametri di tale innovazione è il Piano Provinciale Scuola Digitale (PPSD), un atto programmatico teso a sviluppare e migliorare le competenze digitali dei docenti e degli studenti del Sistema Educativo Provinciale, con particolare riguardo all'utilizzo critico e consapevole dei servizi di Rete e dei mezzi di comunicazione sociale, in modo tale da rendere la tecnologia digitale uno strumento didattico di costruzione delle competenze.

Per lo sviluppo del Piano Scuola Digitale è stata istituita per questo la figura di un animatore a cui si intende attribuire uno dei ruoli strategici per la diffusione dell'innovazione digitale nel settore dell'Istruzione.

Anche nel nostro Istituto è presente questa nuova figura di sistema, l'animatore digitale appunto, che sta iniziando a diffondere le pratiche e i principi contenuti nel PPSD attraverso:

- la formazione interna:
- le attività di animazione digitale nelle classi delle scuole dell'Istituto
- la formazione digitale per i docenti dei due ordini di scuola
- gli sportelli tecnici di accompagnamento individuale rivolti ai docenti dei due ordini di scuola
- il coinvolgimento della comunità scolastica con partecipazione agli incontri di Rete e progetti che vedono coinvolti diversi attori: studenti, famiglie e agenzie del territorio per la realizzazione di una cultura digitale condivisa
- la creazione di soluzioni innovative con:
    - l'individuazione di soluzioni metodologiche e tecnologiche sostenibili da diffondere all'interno degli ambienti della scuola
    - la creazione di re-position personalizzate per condivisione di materiali digitali, app e tools per studenti e docenti
    - la valutazione dei bisogni e delle azioni da intraprendere in collaborazione con il dirigente scolastico
    - la valutazione e la partecipazione ad eventuali bandi digitali.

Obiettivi educativi	Sviluppare negli alunni competenze di accesso ai nuovi linguaggi informatici Stimolare l'utilizzo personale degli applicativi più diffusi nel mondo digitale Potenziare l'utilizzo consapevole delle nuove tecnologie multimediali Sviluppare il pensiero computazionale Sviluppare la capacità di utilizzare in modo responsabile il Web e i nuovi strumenti multimediali emergenti
Destinatari	Alunni dell'Istituto Comprensivo.

Competenze disciplinari	Gli strumenti multimediali consentono di lavorare attraverso un modello interdisciplinare che permette all'alunno di entrare in contatto con nuovi linguaggi e di costruire percorsi creativi e avvincenti in ogni ambito disciplinare: Favorire l'apprendimento di strategie e di abilità finalizzate allo sviluppo delle competenze Sviluppare e consolidare abilità linguistiche Sviluppare e consolidare il pensiero logico Sviluppare abilità manuali e operative Trasformare una situazione complessa in ipotesi di soluzioni possibili (problem solving) Interagire con i compagni, in un piccolo gruppo, organizzando il lavoro e collaborando attivamente per il raggiungimento di un obiettivo comune
Competenze trasversali	Sostenere la motivazione intrinseca Favorire una coerente e adeguata interazione fra lo strumento e l'alunno Sostenere una partecipazione attiva Sviluppare capacità di ricerca Introdurre nuove procedure di organizzazione del lavoro Potenziare la coordinazione oculo-manuale Potenziare la concentrazione e la memoria Favorire la creatività Potenziare la cooperazione e la collaborazione
Sintesi delle attività previste	Laboratorio di informatica per le classi quarta e quinta delle SP Un laboratorio di scratch e robotica educativa della SSPG di Roncone Laboratorio per dsa con software gratuiti: "Leggi per me" e "Project 4s" Laboratorio "A tutto Coding" per SP dell'Istituto Laboratorio di "Robotica educativa" per SP e SSPG dell'Istituto
Risultati attesi	Promuovere l'innovazione della didattica in tutto l'istituto, all'insegna di un reale cambiamento educativo e culturale Garantire l'aggiornamento sulle metodologie didattiche digitali a favore di approcci metodologici aperti Promuovere l'uso dei principali applicativi delle nuove tecnologie Promuovere la gestione dei linguaggi multimediali, potenziando la capacità comunicativa e le abilità sociali, oltreché la creatività

	Favorire il pensiero computazionale
Modalità di verifica	Attività di verifica: Prove pratiche Monitoraggio in itinere Partecipazione utenza Prodotti /artefatti finali Valutazione progetti dai consigli di classe
Valutazione	Criteri di valutazione: abilità nell'utilizzare lo strumento multimediale creatività e capacità di personalizzare il lavoro autonomia capacità di collaborare con i coetanei

2.1.1. Peer education tra alunni

L'Istituto intende continuare a promuovere momenti di peer education per cui si proseguirà con la formazione di alunni e alunne che vogliano assumere il ruolo di figure di riferimento. Saranno gli alunni e le alunne formate durante il secondo anno di SSPG a coinvolgere i compagni ad assumere tale ruolo e a formarli con la supervisione dei docenti referenti.

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

L'Animatore digitale propone percorsi di formazione riguardanti l'utilizzo di metodologie multimediali nella didattica quotidiana progettati a partire dai bisogni dei docenti. L'Animatore digitale supporta durante l'anno scolastico i docenti che utilizzano le TIC con percorsi di sostegno e/o approfondimento individuali o in piccolo gruppo.

La scuola assicura inoltre tempestiva e capillare informazione su corsi, convegni e seminari che riguardino tali argomenti e può aderire a progetti di formazione e accompagnamento curati da enti e associazioni, come già avvenuto in passato.

2.3. Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità

L'Istituto ritiene che le famiglie abbiano due compiti importantissimi: accompagnare e supervisionare i figli durante la navigazione in rete e aiutarli a riconoscere ed evitare i rischi. Queste azioni devono essere condivise con la scuola al fine di garantire la sicurezza di tutti

e la prevenzione di abusi e utilizzi illeciti. A tale scopo sono organizzati incontri informativi e formativi curati da personale competente (Polizia Postale, Carabinieri, esperti di sicurezza in Internet e nuove tecnologie ecc.) e viene suggerita la consultazione dell'Area Genitori del portale Generazioni Connesse dove è possibile reperire informazioni e consigli pratici per un'equilibrata e consapevole gestione del rapporto tra bambini, ragazzi e media.
Saranno inoltre attivati momenti tra rappresentanti dei genitori e referenti per la condivisione della E-Policy e del Patto di corresponsabilità.

3. Gestione dell'infrastruttura e della strumentazione TIC della e nella scuola

3.1. Protezione dei dati personali.

L'Istituto Comprensivo di Tione si appoggia per la sua sicurezza in Rete alla ditta BENASSI s.r.l. DPA CLOUDFABRIC -Via del Commercio 23 – 38121 TRENTO.
Punti chiave:

- sistemi di autenticazione e assegnazione delle risorse;
- server;
- client;
- dispositivi di sicurezza;
- struttura di rete;
- posta e sistemi collaborativi;

3.2. Autenticazione e risorse

L'Istituto dispone di un sistema di autenticazione degli utenti basato su Microsoft Active Directory. Ogni utente (sia esso studente o docente) ha credenziali personali per accedere al sistema informatico di istituto. Le stesse credenziali possono essere utilizzate per accedere ai plessi di Tione, Roncone e Bondo (facenti parte di uno stesso dominio), mentre Ragoli e Zuclo sono due domini indipendenti.
Ad ogni utente viene messa a disposizione una cartella personale sul server accessibile solamente dall'utente stesso e una di scambio, accessibile da studenti e docenti. I docenti hanno a disposizione un'ulteriore cartella di scambio per il materiale da condividere con i colleghi. Tutte queste cartelle sono accessibili da ogni postazione del singolo plesso.
Nel caso vengano riscontrate anomalie nell'utilizzo dello spazio server, possono essere effettuati dei controlli per verificare l'utilizzo lecito del sistema.

Le password degli utenti non hanno scadenza: nel caso di classi che frequentano poco i laboratori informatici e/o con i più piccoli, la scadenza delle password comportava frequenti interventi di ripristino delle stesse con, nella pratica, l'impossibilità di fruire in modo adeguato dei laboratori.
Ad inizio anno scolastico, i nuovi utenti vengono inseriti a sistema tutti con la stessa password. Viene lasciato alla discrezionalità del docente valutare quando invitare gli studenti a procedere alla modifica della stessa. La modifica della password iniziale attiva i servizi G Suite for Education associati all'utente.

3.3. Server

Per garantire stabilità del sistema e velocità di accesso ai dati anche in condizioni di connettività Internet limitata o assente, in ogni plesso è installato un server fisico sul quale vengono memorizzati i documenti del plesso stesso e che gestisce l'autenticazione in replica o in modalità stand-alone (come descritto al punto precedente).
Ogni server ha un sistema RAID (1 o 5, con disco di sicurezza hot spare) per fornire una minima tutela dei dati ivi memorizzati. Per contenere i costi, i sistemi di backup dei plessi sono stati però progressivamente dismessi, e sostituiti da Google Drive (con spazio illimitato) tramite G Suite for Education. Attualmente l'unico backup su NAS attivo è quello della sede di Tione.

3.4. Client

I sistemi operativi in uso all'interno dell'istituto sono vari. Su nessuno di essi gli utenti (ad eccezione del tecnico di laboratorio) hanno permessi amministrativi e le credenziali di dominio funzionano su tutti i client. Per quanto riguarda le differenze tra i sistemi, possiamo dividere i client in due macro-gruppi:

- Le postazioni Windows (7 o 10) hanno installato un sistema antivirus e gli aggiornamenti vengono installati automaticamente.
- Sulle postazioni Linux gli aggiornamenti vengono pianificati dopo averne verificato la stabilità/necessità, e non hanno sistemi antivirus (fortunatamente, il rischio che un client linux venga infettato da malware è ancora piuttosto basso).

Queste postazioni possono essere reinstallate in pochi minuti sfruttando un apposito server di distribuzione (disponibile nei plessi ove è in funzione questo tipo di client).

3.5. Dispositivi di sicurezza

La rete è messa in sicurezza tramite un UTM Cyberoam / Sophos installato in ogni plesso. Questi dispositivi fungono da Antivirus perimetrale, sistema anti intrusione IPS, e forniscono

filtraggio della navigazione, impedendo l'accesso più o meno volontario da parte degli utenti a siti non idonei.

3.6. Rete cablata e WiFi

L'accesso alla rete non è vincolato a protocolli di sicurezza (quali ad esempio 802.1x).

Le porte di rete vengono abilitate semplicemente connettendole nei locali tecnici. Connettendo un dispositivo personale alla rete cablata è quindi possibile navigare in internet (con le limitazioni e le protezioni viste nel paragrafo Dispositivi di sicurezza).

L'accesso alla rete WiFi è consentito ai dispositivi di proprietà dell'istituto e, dietro richiesta effettuata al tecnico, anche su quelli personali. A breve i dispositivi personali dovranno essere connessi ad una rete separata da quella didattica, con il solo accesso ad internet.

Recentemente è stata attivata connettività in fibra, fornita da Trentino Network, in tutti i plessi, ad esclusione di Ragoli.

3.7. Posta e sistemi collaborativi

Da alcuni anni l'istituto ha messo a disposizione di alunni ed insegnanti la piattaforma G Suite for Education.

I documenti importanti possono essere quindi archiviati (e prodotti/modificati) in Drive, la posta di istituto è gestita in Gmail, e Google Classroom è abilitato per tutti gli utenti.

Per tutelare gli alunni, le comunicazioni via mail sono limitate all'interno dell'istituto e con i fornitori di alcuni servizi didattici (salvo classi espressamente autorizzate ad un utilizzo completo della posta).

Le password di accesso a G Suite sono sincronizzate con il dominio principale dell'istituto: le procedure di ripristino password via web sono disabilitate (e non è quindi possibile forzarle dall'esterno).

3.8. Sito Web istituzionale

Il webmaster ALMACREA e i collaboratori interni gestiscono le pagine del sito ed è loro responsabilità garantire che il contenuto sia accurato e appropriato. L'Istituto detiene i diritti d'autore dei documenti che si trovano sul sito e di quei documenti per i quali è stato chiesto ed ottenuto il permesso dall'autore proprietario. La scuola non pubblicherà le fotografie degli alunni. Può essere pubblicato nell'area riservata il materiale didattico prodotto con gli alunni.

Attraverso il proprio sito web la scuola offre:

- informazioni sull'Istituto
- piano dell'offerta formativa
- regolamento di Istituto

- regolamenti di disciplina
- patto educativo di corresponsabilità
- documento di e-policy
- elenco libri di testo in adozione
- nome dei rappresentanti di classe e del Consiglio dell'Istituzione
- amministrazione trasparente
- albo pretorio

3.9. Piattaforma AVAC (Area Virtuale di Apprendimento Cooperativo)

AVAC è stato adottato dall'IC Tione nel 2011 quale piattaforma digitale a supporto delle attività didattiche d'aula.

AVAC è concepito come piattaforma digitale collaborativa in grado sia di condividere documenti e file multimediali, per metterli a disposizione dei discenti 'in qualsiasi momento e in qualsiasi luogo', sia di favorire lo sviluppo e il potenziamento di competenze trasversali, in particolar modo le competenze digitali, che consistono nel padroneggiare le tecnologie telematiche, dell'informazione e della comunicazione, per l'attività di studio, per il tempo libero e per la comunicazione. Uno dei punti di forza di AVAC è la spiccata personalizzabilità dell'ambiente virtuale (Classroom non è personalizzabile): i corsi che contengono i materiali digitali possono essere graficamente adattati e resi motivanti e significativi per gli alunni; i materiali digitali possono essere inseriti tramite link, tramite 'embed', organizzati in cartelle e in tanti altri modi, sfuggendo così alla logica di fredde 'liste' o 'elenchi' di materiali. Le pagine dei corsi assomigliano molto a dei libri in cui immagini, elementi multimediali, testi e altri asset possono essere organizzati per andare incontro alle esigenze cognitive degli alunni. Per tutti questi motivi, soprattutto nelle classi della Scuola secondaria di I grado, viene utilizzato al posto del libro cartaceo per trasferire nell'ambiente digitale una fonte di conoscenza alternativa e versatile.

3.10. Registro elettronico

Dall'anno scolastico 2022-2023 l'istituto ha adottato il registro elettronico ISI-REL. L'accesso al registro, come servizio web delle pubbliche amministrazioni, dovrà avvenire mediante l'utilizzo di strumenti di identità digitale SPID, CIE e CNS/CPS, come previsto dal DL n. 76 del 16.07.2020, convertito con modificazioni dalla legge n. 120 del 11.09.2020.

Il registro elettronico permette ai docenti di svolgere tutte le funzioni istituzionali: registrazione delle presenze in classe, degli argomenti delle lezioni svolte, dei compiti assegnati e delle valutazioni date alle prestazioni degli alunni e delle alunne.
Permette ai genitori di avere in tempo reale tutta una serie di informazioni che riguardano la vita dei propri figli a scuola, di prenotare i colloqui con gli insegnanti, giustificare assenze e ritardi, autorizzare i propri figli a partecipare a progetti e ad uscite didattiche.
Le schede di valutazione intermedie e di fine anno sono visionabili dai genitori al termine degli scrutini.

3.11. Strumentazione personale

Le indicazioni contenute nel Piano Nazionale per la Scuola Digitale e nel successivo Piano provinciale per la Scuola Digitale suggeriscono la necessità di aggiornare il Regolamento d'Istituto in vigore. Premesso ciò, ad oggi ci si attiene alle disposizioni di seguito illustrate, relative alle diverse categorie di persone che agiscono in ambito scolastico: studenti, docenti e personale ATA.

3.11.1. Studenti

Il Regolamento d'Istituto (art. 5, lettera C), recependo il D.P.R. n.249/1998 (Statuto degli studenti e delle studentesse) e la Direttiva ministeriale n. 30 del 15/3/2007, vieta l'uso di cellulari e/o di altri dispositivi elettronici durante le attività didattiche (all'interno o all'esterno.
La scuola garantisce agli alunni e alle alunne, in caso di necessità e su autorizzazione dei docenti, di poter utilizzare il telefono della scuola.
Per specifiche attività didattiche autorizzate dai docenti ed indicate nel loro registro, agli alunni è consentito l'uso di dispositivi mobili personali sotto stretta sorveglianza dei docenti stessi.
Se gli alunni e le alunne sono sorpresi ad usare il telefono durante l'orario scolastico senza autorizzazione, se ne dà comunicazione al dirigente scolastico e ai genitori.

3.11.2. Docenti

Anche i docenti sono tenuti a rispettare il Regolamento d'Istituto e le disposizioni interne relative all'uso dei dispositivi e della rete. Ad essi è affidata la responsabilità dell'accesso a Internet tramite i dispositivi a disposizione durante il proprio orario di servizio (Disciplinare per l'utilizzo della rete internet, della posta elettronica, delle attrezzature informatiche e telefoniche – Delibera della Giunta Provinciale n. 1037 del 7 maggio 2010).

I docenti possono usare i dispositivi personali in orario scolastico solo a scopo didattico e per la compilazione del registro elettronico.

3.11.3. Personale della scuola

Anche il personale ATA è tenuto a rispettare il Regolamento d'Istituto e le disposizioni interne relative all'uso dei dispositivi e della rete. La responsabilità dell'accesso a Internet tramite i dispositivi a disposizione durante il proprio orario di servizio è regolata dal Disciplinare per l'utilizzo della rete internet, della posta elettronica, delle attrezzature informatiche e telefoniche – Delibera della Giunta Provinciale n. 1037 del 7 maggio 2010.

4. Rischi on line: conoscere, prevenire e rilevare[2]

È importante affrontare i principali rischi connessi ad un uso distorto delle tecnologie digitali. La logica del "*controllo*", infatti, soprattutto in una condizione di connessione costante e sempre più personale mediante lo smartphone, risulta inefficace oltre che quasi impossibile da realizzare. Puntare su prevenzione e sensibilizzazione è di certo l'arma migliore per affrontare le problematiche connesse alle TIC.

4.1. Cyberbullismo: che cos'è e come prevenirlo

Il cyberbullismo è una forma di prepotenza virtuale attuata attraverso l'uso di internet e delle tecnologie digitali. Come il bullismo tradizionale è una forma di prevaricazione e di oppressione reiterata nel tempo, perpetrata da una persona o da un gruppo di persone più potenti nei confronti di un'altra percepita come più debole, in genere nel gruppo dei pari.

Il cyberbullismo è un fenomeno differente rispetto al bullismo tradizionale e ha definizioni e caratteristiche proprie.

[2] Le indicazioni dei rischi on-line sono tratte dal sito "generazioniconnesse.it"

Le condotte aggressive online assumono particolari connotati che differenziano il bullismo in rete da quello tradizionale.

Possiamo parlare di cyberbullismo solo se l'atto è:

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

b) **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. Inoltre, la stessa natura del cyberbullismo e il fenomeno della viralità in rete rende molto probabile la ripetitività del danno alla vittima.

c) **dannoso**: la vittima deve percepire il danno psicologico e morale che le viene inflitto;

d) **messo in pratica attraverso computer, cellulari e dispositivi elettronici**: l'uso delle tecnologie digitali è il primo elemento distintivo fra bullismo e cyberbullismo.

Per prevenirlo è efficace 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.

E allora diventa sempre più urgente aiutare i minori a rispondere ad alcune domande cruciali quali: come posso gestire la mia identità nei social network? In che modo posso coniugare le mie esigenze di visibilità con il mio bisogno di tutelare la privacy e la mia sicurezza online? Fino a che punto posso fidarmi dell'autenticità delle informazioni che gli utenti condividono online? Ci sono indizi che possono corroborare la mia fiducia negli altri quando sono online? Come si riconfigurano le relazioni e gli affetti in ambienti saldamente ancorati all'idea di "essere sempre connessi"?

4.2. Hate speech: che cos'è e come prevenirlo

"L'incitamento all'odio (hate speech) 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).

Perché è importante parlarne in classe?

1. È fondamentale che ragazzi e ragazze si rendano sempre più conto della complessità dell'abitare i mondi virtuali. Il piacere del raccontarsi e del mostrare esperienze e

competenze, le nuove amicizie, i diari collettivi che si costruiscono a partire dai tanti post condivisi non sono la sola faccia della medaglia. Bullismo, discorso d'odio, razzismo, offese sono fenomeni che sempre più si è chiamati a gestire. La responsabilità individuale deve attivarsi, occorre rinforzare la costruzione di un'etica delle relazioni.

2. Le rappresentazioni mediatiche influenzano le percezioni pubbliche e i comportamenti, in particolare per argomenti sensibili come le migrazioni ed è quindi importante essere consapevoli degli effetti del flusso di informazioni, specialmente sul web.

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.

Si cerca di rispondere al bisogno degli insegnanti di trovare delle idee per 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)

4.3. 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).

Si tratta di un fenomeno studiato da diversi anni, ma la sua individuazione è molto complessa. Diversi studi permettono di definire 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.

Indicazioni operative

Se si ravvisa un rischio per il benessere psicofisico delle persone minorenni sarà opportuno rivolgersi ad un servizio deputato ad offrire un supporto psicologico anche passando per

una consultazione presso il medico di base o il pediatra di riferimento. Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza (consultori familiari, servizi di Neuropsichiatria Infantile, centri specializzati sulle dipendenze, etc.).

4.4. Gioco online

Il videogioco è un gioco gestito da un dispositivo elettronico che consente di interagire con le immagini di uno schermo. È presente su differenti supporti e il loro utilizzo è sempre più diffuso ed assiduo tanto da diventare parte integrante della vita di bambini e adulti, con la conseguente diffusione di prodotti sempre più complessi e intriganti.

Sono stati individuati aspetti positivi legati ai videogiochi:

a) contribuiscono allo sviluppo di abilità tecniche e strategiche;

b) migliorano la coordinazione oculo-motoria;

c) contribuiscono all'acquisizione di abilità di problem solving.

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

a) la dipendenza legata ad un loro uso eccessivo, con il rischio di trascurare lo studio e le relazioni amicali;

b) 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);

c) i rischi di subire violazioni della privacy

d) contatti indesiderati nei casi di videogiochi online;

e) esposizione a contenuti potenzialmente dannosi;

f) rischio di virus e malware sui dispositivi (a causa di app infette) e di phishing;

Il gioco d'azzardo online, che è cosa diversa dal videogioco, in molti casi sfugge alle restrizioni di età vigenti del 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.

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 [3] ed ai descrittori di contenuto presenti.

4.5. Sexting

Il termine sexting indica 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 semi-nudi (Levick & Moon 2010).
Sue caratteristiche , principalmente, sono:

- **la fiducia tradita**: chi produce ed invia contenuti sessualmente espliciti ripone fiducia nel destinatario, credendo inoltre alla motivazione della richiesta (es. prova d'amore richiesta all'interno di una relazione sentimentale);
- **la pervasività** con cui si diffondono i contenuti: in pochi istanti ed attraverso una condivisione che diventa virale, il contenuto a connotazione sessuale esplicita può essere diffuso ad un numero esponenziale ed infinito di persone e ad altrettante piattaforme differenti. Il contenuto, in tal modo, diventa facilmente modificabile, scaricabile e condivisibile oltre che rendere la sua trasmissione incontrollabile;
- **la persistenza del fenomeno**: il materiale pubblicato on line, può permanervi per un tempo illimitato e potrebbe non essere mai definitivamente rimosso. Un contenuto ricevuto, infatti, può essere salvato, a sua volta re-inoltrato oppure condiviso su piattaforme diverse da quelle originarie e/o in epoche successive.

Generalmente, si usa fare sexting per essere più visibili, desiderabili e accettati socialmente, soprattutto per le ragazze che, attraverso selfie e le immagini provocanti, vogliono apparire più sexy ed attraenti. Per i ragazzi, invece, lo scambio di video e contenuti hard è strumento per mettere in evidenza il proprio potere maschile e le abilità da seduttori.
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 pre-adolescenza e in adolescenza.

[3] Il Pan European Game Information è il metodo di classificazione valido su quasi tutto il territorio europeo usato per classificare i videogiochi attraverso cinque categorie di età e otto descrizioni di contenuto. Ha sostituito altre classificazioni come l'ELSPA dall'aprile 2003.

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.

Esso può verificarsi attraverso la chat (ad esempio, quelle all'interno dei giochi online) e i social network e può condurre ad una relazione sessuale praticata attraverso la webcam o in live streaming e persino a incontri dal vivo fra il minore e l'adulto abusante.

Un minore che viene adescato online corre il serio rischio di un abuso sessuale in un incontro dal vivo.

L'abusante può ottenere immagini o video del minore intime o a sfondo sessuale. Tale materiale potrebbe essere usato per ricattare il minore, venduto, scambiato o potrebbe essere diffuso online distruggendo la reputazione della vittima.

Si possono verificare ripercussioni psicologiche sulla vittima, anche nel caso in cui non si verifichi nessun contatto fisico fra l'adescatore e la vittima.

5. Segnalazione e gestione dei casi

Laddove il docente colga possibili situazioni di disagio connesse ad uno o più di uno tra i rischi elencati nel paragrafo "Prevenzione", dovrà informare il Dirigente Scolastico anche attraverso la compilazione di una "Scheda di segnalazione" (Allegato 3). La scheda di segnalazione potrà essere redatta dal docente sia sulla base di eventi osservati direttamente a scuola, sia su eventi particolari che gli sono stati confidati dall'alunno/a o comunicati da terzi.

A seguito della segnalazione, il Dirigente Scolastico, coinvolto il gruppo di lavoro, avrà cura di contattare il docente per un colloquio finalizzato a valutare la necessità di effettuare uno o più momenti 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 del professionista responsabile dello *Sportello di Ascolto* attivo in istituto, di attori esterni quali le forze dell'ordine e i servizi sociali.

Approvato dal Consiglio dell'istituzione nella seduta del 19 ottobre 2022

ALLEGATI

ALLEGATO.1 – REVISIONE E MODIFICHE DELLA E-POLICY

Nome	E-Safety Policy I.C Tione di Trento
Versione	1.0
Data	GG/MM/AAAA
Autore	Nome del docente responsabile della sicurezza online
Approvato dal Dirigente	
Approvato dal Collegio Docenti	
Prossima data di revisione	

Modifica			
Versione	Data	Descrizione	Nome del docente responsabile della sicurezza online
0.1			
0.2			
0.3			
0.4			

ALLEGATO 2 – MONITORAGGIO SEGNALAZIONI E SANZIONI

ANNO	NUMERO DI SEGNALAZIONI	NUMERO DI INFRAZIONI	NUMERO DI SANZIONI DISCIPLINARI
A.S. …./….			

ALLEGATO 3 Scheda di segnalazione

Scheda di segnalazione		
Alunno/a:		Classe
Problemi evidenziati		
Osservazione diretta	**Evento riferito**	**Descrizione**
		Esposizione a contenuti violenti
		Uso di videogiochi diseducativi
		Utilizzo di informazioni scorrette o pericolose
		Utilizzo di virus per infettare i dispositivi
		Possibile adescamento
		Cyberbullismo (rischio di molestie e maltrattamenti dai coetanei)
		Sexting (scambio di materiale a sfondo sessuale)
		Dipendenza da uso eccessivo della Rete
Firme dei docenti coinvolti	_____ _____	_____ _____

ALLEGATO 4 Patto di corresponsabilità per l'educazione digitale

(estrapolato dal patto di corresponsabil IC Tione che viene firmato da genitori e alunni)

L'INSEGNANTE HA IL DOVERE DI:

- prevedere l'utilizzo degli strumenti digitali all'interno della sua attività didattica per sostenere gli apprendimenti;
- aiutare a sviluppare le competenze digitali previste nel DigCompEdu 2.1;
- vigilare sull'utilizzo appropriato delle tecnologie digitali e di Internet a scuola, nel rispetto della protezione dei dati e delle immagini personali degli alunni e delle alunne;
- educare gli studenti ad un utilizzo responsabile delle tecnologie e ad una comunicazione rispettosa degli altri anche in rete (Netiquette);
- aiutare gli alunni e le alunne in caso di difficoltà nell'utilizzo delle tecnologie digitali, supportandoli in caso di abuso e condotta non adeguata, attuando le procedure descritte nel documento e-policy, assicurandosi che gli studenti sappiano a chi rivolgersi per segnalare eventuali abusi.

L'ALUNNO/A HA IL DIRITTO DI:

- utilizzare gli strumenti digitali all'interno della sua attività didattica per sostenere gli apprendimenti;
- essere aiutato a sviluppare le competenze digitali previste nel DigCompEdu 2.1;

L'ALUNNO/A HA IL DOVERE DI:

- utilizzare le tecnologie digitali e i dispositivi mobili solo se autorizzato dai docenti;
- comunicare difficoltà e bisogni nell'utilizzo delle tecnologie digitali a docenti e genitori;
- segnalare abusi e condotte non adeguate rispetto ai contenuti on-line;
- adottare comportamenti rispettosi degli altri anche nella comunicazione in rete;
- prendere consapevolezza che dati e immagini personali possono essere manipolati e usati in maniera lesiva da parte di altre persone.

LA FAMIGLIA HA IL DOVERE DI:

- rendere consapevoli i propri figli delle conseguenze di un uso scorretto di filmati e immagini sensibilizzandoli ai rischi della rete, in modo complementare ai docenti;
- affiancare i docenti nella funzione educativa e vigilare sulle comunicazioni in rete dei ragazzi;
- concordare con i docenti linee di intervento coerenti di carattere educativo in relazione ai problemi rilevati per un uso scorretto o pericoloso della rete.