



Ministero della Pubblica Istruzione
Ufficio Scolastico Regionale per la PUGLIA

Istituto Comprensivo Statale
72020 Erchie (BR)

TRINITY
COLLEGE LONDON
Registered Examination Centre
n. 10031

Scopo della Policy.

La *policy* ha i seguenti scopi:

- a. garantire la formazione degli alunni e del personale scolastico su un uso consapevole delle risorse web, sia in quanto materiale da utilizzare nella didattica, sia in quanto strumento potente per la comunicazione e la socializzazione;
- b. dare indicazioni per la validazione dei contenuti e delle notizie incrociando fonti diverse;
- c. prevenire o quantomeno ridurre al minimo atti e condotte che possano configurarsi come reati;
- d. prevenire l'esposizione a contenuti e siti web inappropriati;
- e. fornire modalità per la tutela della reputazione e dei dati personali on-line anche per evitare il furto d'identità;
- f. tutelare la salute e il benessere educando a una navigazione di qualità e di durata non eccessiva;
- g. predisporre azioni educative per prevenire fenomeni di grooming, sexting, bullismo e cyberbullismo;
- h. contenere chiare indicazioni e linee guida per regolamentare il comportamento degli studenti nelle aule

scolastiche e negli altri ambienti dell'istituto;

- i. regolamentare le azioni dei docenti e del personale scolastico che dovessero ravvisare delle violazioni;
- j. definire una catena e rete di azioni da compiere per gestire situazioni critiche del presente documento;
- k. prevedere incontri di formazione per alunni, famiglie e personale scolastico all'inizio dell'anno scolastico;
- l. contenere inoltre la casistica e le modalità di erogazione di sanzioni disciplinari qualora si verificassero comportamenti poco appropriati all'interno della scuola.

Ruoli e Responsabilità

RUOLO	RESPONSABILITA'
Il Dirigente Scolastico	<ul style="list-style-type: none">● assume la responsabilita' generale● garantisce la formazione adeguata del personale riguardante i ruoli di sicurezza online● garantisce l'utilizzo del firewall per filtrare tentativi di connessioni a siti impropri● garantisce verifiche periodiche antivirus● garantisce il controllo periodico del sistema informatico, dei file utilizzati e dei siti visitati dalle macchine● nomina un docente referente della e-safety● garantisce la variazione periodica delle credenziali d' accesso alla connessione wireless● nomina un referente per la sicurezza online in ogni plesso● informa i genitori di eventuali comportamenti inappropriati relativi alla sicurezza online che si verificano all'interno della scuola.

<p>DSGA</p>	<ul style="list-style-type: none"> ● dispone che la scuola utilizzi un firewall o altro sistema di filtri per evitare le connessioni a siti impropri ● assicura la tutela dei dati sensibili in quanto responsabile della loro sicurezza ● dispone verifiche antivirus periodiche sui computer e sui tablet ● dispone il controllo periodico del sistema informatico, dei file utilizzati e dei siti visitati da ogni macchina ● facilita la formazione e la consulenza per tutto il personale ● controlla la condivisione di dati personali ● prevede un responsabile del parco tecnologico che controlli periodicamente la sicurezza della connessione ad internet di tutte le macchine della scuola ● dispone la variazione periodica delle credenziali d'accesso alla connessione wireless nei vari plessi.
<p>docente- referente nominato dal DS</p>	<ul style="list-style-type: none"> ● condivide la responsabilità per i problemi di sicurezza online con i responsabili di plesso ● promuove la consapevolezza e l'impegno per la salvaguardia online in tutta la comunità scolastica ● assicura che l'educazione alla sicurezza online sia incorporata in tutto il programma di studi ● istituisce un registro per i siti visitati da docenti e alunni durante le ricerche online nell'aula multimediale ● coordina interventi educativi e informativi con le autorità locali e le agenzie competenti ● propone l'organizzazione di corsi di formazione per docenti, genitori, operatori del settore socio-educativo ● monitora il fenomeno del cyberbullismo attraverso questionari (allegato n.3 della bozza) ● registra casi di cyberbullismo e bullismo accaduti all'interno dell'ambiente scolastico.

L'Animatore Digitale ed il team dell'innovazione	<ul style="list-style-type: none">● pubblicano la e-safety policy sul sito della scuola;● diffondono la “e-safety policy” attraverso power point, e-book e schede di sintesi;● coadiuvano l’azione del docente referente della sicurezza online● forniscono a docenti e alunni un archivio di risorse online libere dal diritto d’autore.
---	--

I Docenti

- esplicitano obiettivi sulla sicurezza online e inseriscono tematiche correlate in tutte le discipline del curricolo verticale
- guidano gli alunni con cura quando sono impegnati in attività di apprendimento che coinvolgono risorse online
- illustrano ad alunni e genitori il documento di e-safety, che integrerà il patto di corresponsabilità, e si accertano che venga sottoscritto
- effettuano il logout per uscire da account personali o piattaforme educative
- garantiscono che gli alunni siano pienamente consapevoli delle capacità di ricerca e delle leggi sul copyright
- utilizzano sistemi di archiviazione cloud del materiale didattico per evitare l'uso di chiavette usb, cd e dvd personali
- informano il responsabile di plesso sugli episodi di cyberbullismo, sexting, grooming o qualsivoglia comportamento inappropriato di sicurezza online
- partecipano a convegni, incontri e seminari sul tema del bullismo e del cyberbullismo
- presentano e fanno sottoscrivere tempestivamente alle famiglie dei nuovi iscritti e di tutti gli alunni che arrivano durante l'anno scolastico, il patto di corresponsabilità e la liberatoria per l'utilizzo di dati e immagini personali a scopo didattico
- prevedono misure di sostegno e di rieducazione degli alunni coinvolti in episodi di cyberbullismo
- pubblicano il materiale didattico prodotto su piattaforme educative, sul sito o sul canale youtube della scuola, previo accertamento delle liberatorie da parte dei genitori e nel rispetto delle leggi sul copyright.

Il personale ATA	<ul style="list-style-type: none"> ● è consapevole dei problemi di sicurezza on-line connessi con l'uso di telefoni cellulari, fotocamere e dispositivi portatili ● vigila sull'uso inadeguato di telefonini, fotocamere e dispositivi portatili da parte degli alunni nei momenti in cui non sono sotto la vigilanza diretta dei docenti ● segnala qualsiasi abuso sospetto o problema ai responsabili della sicurezza online ● adotta comportamenti sicuri, responsabili e professionali nell'uso della tecnologia ● partecipa a convegni, incontri e seminari sul tema del bullismo e del cyberbullismo.
Gli alunni	<ul style="list-style-type: none"> ● leggono, comprendono, accettano e sottoscrivono la e-safety policy ● si impegnano ad acquisire una adeguata capacità di ricerca e selezione delle risorse online ● comprendono la necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore ● comprendono l'importanza di segnalare tempestivamente abusi o usi impropri o l'accesso a materiali inappropriati ● riferiscono ai docenti episodi di bullismo o cyberbullismo ● riconoscono l'importanza di un uso corretto di telefoni cellulari, fotocamere digitali e dispositivi portatili ● chiudono la connessione alla fine di ogni collegamento ● effettuano il logout per uscire da account personali o piattaforme educative ● capiscono l'importanza delle regole sull'uso di immagini e dati personali ● conoscono le sanzioni previste per l'uso improprio di dispositivi tecnologici personali o della scuola ● comprendono l'importanza di adottare buone pratiche di sicurezza on-line quando si usano le tecnologie digitali fuori dalla scuola ● utilizzano sistemi di archiviazione cloud del materiale didattico per evitare l'uso di chiavette usb, cd e dvd personali ● partecipano a convegni, incontri e seminari sul tema del bullismo e del cyberbullismo organizzati dalla scuola ● riconoscono i rischi dell'utilizzo di internet e di altre tecnologie a scuola e a casa.

<ul style="list-style-type: none"> ● I genitori 	<ul style="list-style-type: none"> ● sostengono la scuola nel promuovere la sicurezza online e approvano, per mezzo dei propri rappresentanti in consiglio d'istituto, l'accordo di e-safety policy dell'istituto; ● leggono e controfirmano il paragrafo, riguardante le responsabilità delle varie componenti, che diventerà parte integrante del patto di corresponsabilità. ● leggono e controfirmano il patto di corresponsabilità all'atto dell'iscrizione nel momento in cui dovesse avvenire ad anno scolastico in corso ● accedono al sito web della scuola in conformità con quanto stabilito dalla stessa; ● partecipano a convegni, incontri e seminari sul tema del bullismo e del cyberbullismo organizzati dalla scuola.
--	--

Condivisione e comunicazione della Policy all'intera comunità scolastica.

La E-Safety Policy d'Istituto si applica a tutti i membri della scuola: il personale docente e non, gli studenti, i genitori, gli utenti della comunità.

E' compito del Dirigente Scolastico approvarla, previa condivisione e approvazione degli organi collegiali, disporre la pubblicazione per una conoscenza diffusa sul sito della scuola e sottoscriverla insieme alle famiglie tramite il Patto di Corresponsabilità.

Tale documento sarà sottoposto a revisione periodica con cadenza almeno annuale, possibilmente all'inizio di ogni anno scolastico in concomitanza con l'aggiornamento della check list sulla sicurezza, e comunque ogni qualvolta si ritenga necessario per sopraggiunte revisioni della normativa che disciplina la materia.

Gestione delle infrazioni alla Policy:

La scuola prenderà tutte le precauzioni necessarie per garantire la sicurezza on-line anche se, a causa della portata globale dei contenuti WEB e la disponibilità di tecnologie mobili anche personali, sarà difficile avere un controllo diretto sulla totalità degli alunni e delle loro azioni.

Al personale e agli alunni saranno date informazioni sulle infrazioni in uso e sulle eventuali sanzioni.

Le suddette sanzioni includono:

- ritiro del cellulare fino a fine giornata e consegna ai genitori da parte del dirigente o di un suo delegato;
- divieto di utilizzo delle tecnologie multimediali per un periodo da concordare con la famiglia;
- comunicazione alle autorità competenti nei casi di gravi infrazioni o atti che si configurano come cyberbullismo.

1. Monitoraggio dell'implementazione Policy e suo aggiornamento

La E-Safety Policy si inserisce all'interno del nostro Istituto Comprensivo al fine di proteggere i minori da episodi di bullismo o cyberbullismo e per garantire il benessere degli alunni a scuola e negli ambienti di vita quotidiana.

Il Comprensivo avrà un docente referente per il bullismo e il cyberbullismo supportato dai referenti di ogni plesso.

La E-Safety Policy sarà riesaminata annualmente o quando si verificano cambiamenti significativi per quanto

riguarda le tecnologie in uso all'interno della scuola e tutte le modifiche della Policy saranno conformi alle direttive presenti nella legge 71 del 29 maggio 2017 (G.U. del 3 giugno 2017).

2. Formazione e Curricolo

Il Piano Nazionale Scuola Digitale (PNSD) ha l'obiettivo di modificare gli ambienti di apprendimento per rendere l'offerta formativa di ogni istituto coerente con i cambiamenti della società della conoscenza e con le esigenze e gli stili cognitivi delle nuove generazioni.

Il PNSD e le azioni in esso previste hanno consentito di innovare il nostro Comprensivo dotandolo di strutture e dotazioni tecnologiche e di tutte le figure professionali necessarie all'innovazione digitale nella scuola.

Utilizzando risorse economiche dei fondi regionali abbiamo, inoltre, istituito corsi di formazione per personale docente e ATA sulle metodologie didattiche innovative.

Nell'ambito del PNSD questa scuola ha previsto:

- individuazione e formazione di un Animatore Digitale che come docente accompagna il Dirigente Scolastico, il Direttore S.G.A. e il personale docente nell'attuazione degli obiettivi e delle innovazioni previste dal PSND;
- somministrazione di un questionario rivolto ai docenti per la rilevazione dei bisogni "digitali";
- realizzazione/ampliamento della rete WI-FI/LAN dei vari plessi dell'Istituto;
- ricognizione, messa a punto e potenziamento delle dotazioni digitali;

L'Istituto s'impegna a proporre attività mirate a sviluppare una serie di competenze e comportamenti adeguati alle età degli alunni:

1. programmando laboratori di Coding in occasione della Settimana del codice, dell'ora del codice e dell'implementazione di progetti per l'ampliamento dell'offerta formativa;
2. proponendo, a partire dal prossimo anno scolastico, un programma di progressiva educazione alla sicurezza online come parte integrante del curriculum scolastico i cui obiettivi educativi saranno:
 - sviluppare una serie di strategie per indurre l'alunno a valutare e verificare le informazioni prima di accettarne la veridicità;
 - rispettare i principi della Netiquette quando si utilizza un ambiente online;
 - capire il motivo per cui non dovrebbero inviare o condividere resoconti dettagliati delle loro vite personali e informazioni di contatto;
 - capire il motivo per cui non devono pubblicare foto o video di altri senza il loro permesso e non devono scaricare alcun file o utilizzare applicazioni senza il permesso del docente (il quale deve essere autorizzato dal D.S., o in sua assenza dall'animatore digitale o dal responsabile del parco tecnologico, come stabilito nel regolamento per l'utilizzo del laboratorio multimediale);
 - essere unico responsabile della macchina su cui lavora per tutto il periodo di utilizzo (a inizio anno ogni alunno verrà associato ad una macchina del lab. multimediale);
 - utilizzare le fonti e visitare i siti suggeriti dal docente;

- comprendere l'impatto del bullismo online, del sexting, del grooming e sapere come e a chi chiedere aiuto per sé e/o per gli altri.

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

Sicurezza della rete senza fili (Wireless - WiFi)

L'Istituto dispone di una rete con tecnologia senza fili e di reti cablate.

L'ottenimento delle credenziali di accesso alla rete, che saranno modificate periodicamente, è riservato ai docenti e al personale dell'Istituto.

La rete interna dovrà essere protetta da Firewall per quanto riguarda le connessioni con l'esterno.

Le postazioni sono protette con sistemi antivirus che saranno regolarmente aggiornati.

Sito web della scuola

L'Istituto dispone di un sito internet a norma di legge: www.icerchie.gov.it

La scuola, in qualità di ente pubblico, pubblicherà sul proprio sito web i contenuti che saranno valutati come pertinenti alle finalità educative istituzionali, ponendo attenzione alla tutela della privacy degli studenti e del personale, secondo le disposizioni normative. La pubblicazione di eventi o materiale didattico che contengono immagini o dati personali di adulti e alunni avverrà previo accertamento, da parte del docente proponente, delle necessarie autorizzazioni e liberatorie.

4.Strumentazione personale

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

Come da Regolamento d'Istituto agli studenti è vietato l'utilizzo del cellulare all'interno della scuola e come per gli anni precedenti potranno portare a scuola il loro dispositivo solo previa autorizzazione, rilasciata ad inizio anno, da parte dei genitori. Per quanto concerne l'utilizzo dei tablet e pc personali, questi possono essere utilizzati solo alla presenza del docente e per ragioni prettamente scolastiche.

Per i docenti e per il personale della scuola: gestione degli strumenti personali - cellulari, tablet ecc..

I docenti e il personale della scuola possono utilizzare cellulari e tablet a scopo personale non durante l'attività didattica o lavorativa.

5. Prevenzione, rilevazione e gestione dei casi

Prevenzione

Principi generali:

1. Quando si inizia a navigare in rete bisogna informarsi subito su quali sono i diritti e i doveri dell'utente, leggendo il regolamento, tenendosi aggiornati, esplorando i siti informativi e istituzionali che affrontano queste tematiche.
2. Sensibilizzare gli alunni a selezionare con cura che cosa rendere pubblico e cosa rendere privato. E' indispensabile scegliere con attenzione le amicizie con cui accrescere la propria rete e i gruppi a cui aderire, proteggendo la propria identità digitale con password complesse e usando una domanda di recupero password

dalla risposta non banale.

3. E' necessario avere il permesso di ciascun utente coinvolto prima di effettuare la pubblicazione. Evitare di pubblicare su YouTube video girati di nascosto e dove sono presenti persone filmate senza il loro consenso.
4. Ogni abuso subito o rilevato nella navigazione, deve essere segnalato ai genitori e/o ai docenti.

Azioni:

La scuola si impegna a:

- riconoscere il Dirigente Scolastico come titolare del trattamento di dati personali secondo la Legge sulla privacy (art. 41f del D.Lgs. 196/2003);
- riconoscere il DSGA come responsabile della sicurezza dei dati personali;
- riconoscere come responsabili della sicurezza online un docente su nomina del Dirigente Scolastico;
- riconoscere i docenti disciplinari come responsabili della sicurezza online degli alunni ad essi affidati durante le ore di lezione e altre attività a valenza educativo-didattica.

Rilevazione e gestione dei casi

Intervenire efficacemente nei casi di probabile cyberbullismo o adescamento in internet non è semplice. Per questo motivo è necessario ricorrere ad un protocollo ben definito di azioni che esonera il docente dalla libera iniziativa personale (allegato n. 1).

Elenco allegati

- a. Allegato n.1 proposto nei materiali messi a disposizione delle scuole dal sito e dalla piattaforma di “Generazioni connesse” e che propone una rete di figure e azioni per un tempestivo ed efficace intervento nella gestione dei vari problemi;
- b. Allegato n.2, sempre proposto da “Generazioni connesse” è un diario di bordo per la documentazione dei casi che si sono verificati e delle modalità con cui sono stati gestiti anche con lo scopo di migliorare gli interventi successivi;
- c. Allegato n.3, il questionario da somministrare online, garantendo l’anonimato, agli alunni a partire dalla quarta primaria fino alla terza secondaria di primo grado per monitorare il fenomeno del bullismo e del cyber bullismo (ci proponiamo di completare il questionario con quesiti riguardanti il grooming e il sexting); ci proponiamo, inoltre di predisporre, con l’ausilio dei docenti delle prime classi della primaria, un questionario analogo, adeguato all’età dei piccoli alunni;
- d. E’ ancora in fase di definizione l’Allegato n.4 relativo alle procedure operative per la gestione delle infrazioni alla Policy.

Approvato dal Collegio dei Docenti in data 29 giugno 2017

Il Dirigente Scolastico