ISTITUTO PER L'ISTRUZIONE SUPERIORE "GIOVANNI DA VIGO – NICOLOSO DA RECCO"
Liceo classico, linguistico e scientifico – Rapallo, Recco, Chiavari
Sito: www.davigonicoloso.edu.it – Blog studenti: www.sharing.school
Piattaforma e-Learning: www.davigonicoloso.it/moodle29
Via don Giovanni Minzoni 1, 16035 – Rapallo (Ge) - Italy
Mail: geis00100n@istruzione.it – pec: geis00100n@istruzione.pec.it – Tel: 0185.61082

E-Safety School Policy

Indice generale

Introduzione **2**
Scopo della E-Safety Policy 2
Ruoli e Responsabilità 2
Condivisione e comunicazione della Policy all'intera comunità scolastica 2
Gestione delle infrazioni alla Policy 2
Monitoraggio dell'implementazione della Policy e suo aggiornamento 2
Integrazione della Policy con Regolamenti esistenti 2
Formazione e Curricolo **3**
Curricolo sulle competenze digitali per gli studenti 3
Formazione dei docenti sull'utilizzo e integrazione delle TIC nella didattica 3
Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali 3
Sensibilizzazione delle famiglie 3
Gestione dell'infrastruttura e della strumentazione ICT della scuola **4**
Accesso ad internet: filtri, antivirus e sulla navigazione 4
Gestione accessi 4
Sito web istituzionale, piattaforma di e-learning, posta elettronica 4
Blog Company e Social Networks 4
Protezione dei dati personali 4
Strumentazione personale **6**
Corresponsabilità nelle comunicazioni digitali **6**
Netiquette 6
Prevenzione, rilevazione e gestione dei rischi legati all'utilizzo di Internet **8**
Prevenzione 8
Rilevazione 8
Gestione dei casi 8

Introduzione

Scopo della E-Safety Policy

Lo scopo della E-Safety Policy è di presentare le linee guida dell'Istituto in merito all'utilizzo delle tecnologie dell'informazione. Tali tecnologie sono parte della regolare attività didattica nelle aule, sono utilizzate nella comunicazione scuola-famiglia e rivestono un ruolo importante nella vita sociale degli studenti e delle studentesse. Data la pervasività di tali tecnologie, l'Istituto è chiamato non solo a redigere aspettative di comportamento alle quali tutti i membri della comunità scolastica sono chiamati ad attenersi, al fine di garantire un ambiente adeguato all'utenza e sicuro, ma anche ad attivare percorsi di formazione per promuovere un uso responsabile della rete. Opportune azioni disciplinari e/o legali vengono intraprese nel caso di comportamenti inappropriati o addirittura illeciti.
L'Istituto aderisce all'iniziativa "Safer Internet Centre - Generazioni Connesse", co-finanziato dalla Commissione Europea nell'ambito del programma *"Connecting Europe Facility" (CEF)*, attraverso il quale la Commissione promuove strategie finalizzate a rendere Internet un luogo più sicuro per gli utenti più giovani, promuovendone un uso positivo e consapevole.

Ruoli e Responsabilità

Il **Dirigente Scolastico** è responsabile per la sicurezza dei dati, è informato sulle linee guida contenute nella e- policy ed è garante della sua applicazione.
I **Collaboratori del Dirigente** partecipano delle attività di salvaguardia della presente policy, incentivando la riflessione e la progettazione in ottemperanza alle regole qui definite ed offrendo spunti per la sua integrazione e il suo adattamento ai veloci cambiamenti che coinvolgono ed interessano questo settore.
L'**Animatore Digitale** promuove la diffusione dei suoi contenuti.
I **Referenti per il Bullismo e il CyberBullismo** promuovono azioni per la prevenzione del fenomeno.
Il **Responsabile per la Protezione dei Dati** (DPO) è una figura esterna che fornisce consulenza al Dirigente Scolastico e informa tutte le figure coinvolte, sia in merito alla normativa, sia riguardo alle soluzioni tecniche adottate per rispettare gli standard imposti. Al DPO ci si può rivolgere nei casi in cui si prospetti una violazione della privacy nel trattamento dei dati perosnali.
Il tema della sicurezza e dei rischi connessi ad Internet è trattato dai docenti nella didattica, in particolar modo quando essa sia assistita dalle tecnologie digitali.
I **genitori** sostengono la scuola nel promuovere la sicurezza online, leggendo la policy e partecipando agli incontri organizzati dalla scuola sui temi della sicurezza online.
Gli **studenti** conoscono e rispettano la policy e il regolamento di Istituto, segnalando ai docenti eventuali usi impropri della rete e dei dispositivi.

Condivisione e comunicazione della Policy all'intera comunità scolastica

La E-Safety Policy è pubblicata sulla Home Page del sito della scuola dopo essere stata approvata dal Consiglio di Istituto. All'inizio di ogni anno scolastico, insieme al Patto di Corresponsabilità, la E-Policy viene illustrata ai genitori e agli studenti della scuola.

Gestione delle infrazioni alla Policy

Nel caso in cui un docente rilevi un'infrazione alle indicazioni della Policy è necessario che informi il coordinatore di classe, il quale a sua volta riferisce al Dirigente Scolastico e alla famiglia. Nel caso in cui l'infrazione si configuri come atto di cyberbullismo, il docente informa lo staff di Presidenza. Nel caso si configuri l'ipotesi di un reato è necessario che il Dirigente informi le autorità competenti (polizia postale).

Monitoraggio dell'implementazione della Policy e suo aggiornamento

Il Dirigente Scolastico è responsabile dell'implementazione della Policy all'interno dell'Istituto. Lo staff di presidenza e l'animatore digitale, in accordo con il Dirigente Scolastico, partecipano alla revisione e all'aggiornamento del documento. L'aggiornamento del documento viene sottoposto all'approvazione del Consiglio di Istituto.

Integrazione della Policy con Regolamenti esistenti

La Policy è coerente con quanto stabilito dalla Legge (*"Statuto delle studentesse e degli studenti della scuola secondaria" - DPR 24 giugno 1998 n. 249 modificato dal DPR 21 novembre 2007 n. 235"*; *"Disposizioni a tute la dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo" - Legge 29 maggio 2017 n. 71*; *Regolamento Europeo 679/2016 in materia di privacy e protezione dei dati personali*), dai Regolamenti interni vigenti e dal Patto di Corresponsabilità.

Formazione e Curricolo

Curricolo sulle competenze digitali per gli studenti

Tali competenze vengono promosse in maniera trasversale dai docenti, sulla base delle loro pratiche di insegnamento. Al termine del primo e del secondo biennio di studi, le competenze vengono certificate sulla base del quadro comune europeo:

- Primo Biennio: *"usa le tecnologie per interagire con compiti e problemi ben definiti e non sistematici"*
- Secondo Biennio: *"usa le tecnologie per compiti precisi e opportuni con la capacità di adattarsi alle dinamiche presenti in un contesto complesso"*
- Monoennio Finale: *"usa le tecnologie per interagire con problemi complessi nell'ambito di soluzioni limitate, contribuendo alla prassi formativa della comunità in supporto anche alle difficoltà di terzi"*

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

L'Animatore digitale e il referente d'Istituto per la Formazione predispongono un piano di formazione triennale progettato a partire dai bisogni formativi dei docenti. I corsi attivati riguardano l'utilizzo di metodologie didattiche innovative.

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

I docenti sono invitati a partecipare ai seminari di formazione interni che trattino parti legate alla sicurezza interna e all'utilizzo della rete.

Sensibilizzazione delle famiglie

L'Istituto invita i genitori ad assumersi l'incarico di supervisionare i figli durante la navigazione in rete, aiutandoli a riconoscere ed evitare i rischi. Corsi di formazione ad hoc verranno proposti dalla scuola all'intero territorio e alle singole famiglie. La presenza dello psicologo interno alla scuola fa sì che tali proposte si declinino nella formazione individuale dei ragazzi e delle ragazze, mettendo in evidenza rischi e opportunità della vita virtuale.

Gestione dell’infrastruttura e della strumentazione ICT della scuola

Accesso ad internet: filtri, antivirus e sulla navigazione

Nella logica di evitare l’esposizione a contenuti inappropriati e l’accesso a piattaforme potenzialmente dannose e/o particolarmente invasive, i sistemi dell’Istituto sono protetti da firewall con content filtering e accesso a DNS con blacklist. I computer sono dotati di antivirus, monitorati e tenuti aggiornati dai responsabili dei laboratori.

Gestione accessi

L’acceso ai pc, sia nelle aule computer che nelle classi, avviene sempre tramite credenziali gestite dall’Amministrazione. La connessione alla rete wi-fi è riservata ai docenti per fini didattici ed è accessibile solo dietro identificazione personale.

Sito web istituzionale, piattaforma di e-learning, posta elettronica

Il sito del Liceo è raggiungibile all’indirizzo http://www.iisdavigonicoloso.edu.it. Il Dirigente e lo staff verificano i contenuti destinati alla pubblicazione. Responsabile della gestione del sito è il docente designato all’inizio di ogni anno scolastico e segnalato nell’organigramma dell’Istituto.
Le comunicazioni da e verso l’istituto sono veicolate esclusivamente dalla mail istituzionale e dal Registro Elettronico, la cui gestione è direttamente sotto il controllo dell’Istituto su un dominio in hosting.
Tramite una piattaforma di e-learning open source, la cui gestione è direttamente sotto il controllo dell’Istituto su un dominio in hosting, viene gestito un ambiente di Virtual Learning all’interno del quale sono profilati studenti e docenti, con accesso protetto tramite credenziali individuali.

Blog Company e Social Networks

La scuola dispone di una piattaforma denominata “Sharing”, accessibile all’indirizzo www.sharing.school . A partire da tale piattaforma è stato strutturato un progetto di formazione al giornalismo e al marketing che ogni anno viene seguito da un docente designato dal Collegio dei Docenti di settembre e inserito regolarmente nell’organigramma della scuola. Tale progetto si occupa principalmente della gestione del blog informativo denominato appunto “sharing.school”. Sharing si occupa di:

- approfondire e discutere tematiche di attualità nel rispetto dei principi del pluralismo;
- diffondere e raccontare la vita della scuola nel rispetto della privacy del personale e degli studenti in qualità di Blog company collegato all’Istituzione stessa attraverso la responsabilità legale dell’Associazione gestrice;
- approfondire ed esplorare l’uso consapevole dei social media anche in un’ottica di social marketing, ottemperando i meccanismi di una redazione giornalistica digitale e quelli di un social media management finalizzato alla produzione e diffusione di contenuti, nonché alla fidelizzazione degli utenti e all’avvio alle pratiche SEO. A tal proposito va segnalata la presenza del marchio sharing anche su Facebook ed Instagram; ogni autore che posta articoli sul blog deve fornire il proprio consenso (o quello di coloro che esercitano la responsabilità genitoriale se lo studente è minorenne) alla comparsa del proprio nome, della propria immagine e dei propri contenuti digitali sulla piattaforma. Tale autorizzazione può essere previamente concessa all’inizio del progetto per i partecipanti alla redazione, oppure deve essere fornita ad ogni singolo intervento nel caso di studenti non facenti parte della redazione del progetto stesso.

Il link al progetto Sharing è presente sul sito dell’Istituto come accesso a sito esterno.

Protezione dei dati personali

In fase di iscrizione degli alunni alla scuola, è fornita ai genitori un'informativa sul trattamento dei dati personali ai sensi degli artt. 13 e 14 del Regolamento Europeo 679/2016 In occasione di ogni attività è richiesto ai genitori – di cui all’art. 7 del medesimo Regolamento – il consenso all'utilizzo di materiale fotografico e audiovisivo riservato ed elaborati degli alunni per esporli anche in sedi diverse da quelle dell'Istituto quali pubblicazioni in formato digitale e siti web. Nel caso di studenti maggiorenni saranno fornite direttamente le informazioni di cui sopra e saranno direttamente richiesti, ove necessari, i consensi di cui all’art. 7, indipendentemente dalle informazioni rese e dai consensi ottenuti con riguardo a coloro che precedentemente Sul sito dell’Istituto non compaiono né nominativi, né foto, né video in cui sia esplicitamente riconoscibile l’identità di uno degli studenti della scuola.
In caso di utilizzo di piattaforme digitali condivise, di assegnazione indirizzi di posta elettronica istituzionale agli studenti o di strumenti per la creazione e la gestione di classi virtuali viene acquisito preventivamente il consenso informato dei genitori.

In caso di attività di ampliamento dell'offerta formativa, organizzate in collaborazione con Enti esterni, viene richiesto preventivamente ai genitori il consenso informato alle riprese audio/video e rilasciata un'informativa ulteriore – da parte dell'ente esterno coinvolto – circa l'utilizzo dei dati raccolti nella sessione di lavoro/intervento presso i nostri studenti. L'accesso ai dati riportati nel registro elettronico (ritardi, assenze, note e valutazioni) è riservato ai genitori tramite l'invio di una password di accesso strettamente personale.

Strumentazione personale

Per gli studenti: E' vietato l'utilizzo di cellulari e smartphone per l'intera durata delle attività scolastiche (una pausa centrale esclusa). E' consentito agli alunni con Bisogni Educativi Speciali utilizzare il proprio notebook o tablet, senza connessione internet. È consentito a tutti gli alunni, in casi specifici concordati con il docente (uscite didattiche, produzioni multimediali...) l'utilizzo di dispositivi elettronici personali per scopi didattici.

Per i docenti: durante il loro orario di servizio è consentito l'utilizzo di dispositivi elettronici personali solo ed esclusivamente per fini didattici.

Per il personale della scuola: è vietato l'utilizzo di dispositivi elettronici durante l'orario di servizio a meno che non sia funzionale alla mansione chiamata a svolgere nella singola mattinata.

Corresponsabilità nelle comunicazioni digitali

Dati gli obiettivi didattici, pedagogici e lavorativi dell'uso dei sistemi istituzionali di posta elettronica e della piattaforma di e-learning di Istituto, studenti e docenti si impegnano a:

- conservare le password personali e non consentirne l'uso ad altre persone;
- comunicare immediatamente ai tecnici preposti l'impossibilità ad accedere al proprio account o il sospetto che altri possano accedervi;
- non consentire ad altri, a nessun titolo, l'utilizzo della piattaforma di e-learning e del proprio account di posta elettronica;
- non diffondere eventuali informazioni riservate di cui venisse a conoscenza, relative all'attività delle altre persone che utilizzano il servizio;
- utilizzare i servizi offerti solo ad uso esclusivo per le attività didattiche della scuola;
- quando ci si avvale di un PC in modo non esclusivo, utilizzare sempre i browser in modalità *navigazione in incognito*, non memorizzare la password ed effettuare sempre il logout;
- non danneggiare, molestare, insultare altre persone;
- non violare la riservatezza di altre persone o comunque comunicare dati personali;
- non creare e non trasmettere immagini, dati o materiali offensivi, osceni o indecenti;
- non creare e non trasmettere materiale offensivo per altre persone o enti;
- non creare e non trasmettere materiale commerciale o pubblicitario;
- quando si condividono documenti non interferire, danneggiare o distruggere il lavoro altrui;
- rispettare le buone regole della *netiquette* allegata.

Dati gli obiettivi didattici e pedagogici delle lezioni in video-conferenza, gli studenti si impegnano a:

- mantenere strettamente riservato il link di accesso;
- entrare con puntualità nell'aula virtuale;
- partecipare ordinatamente ai lavori che vi si svolgono;
- presentarsi ed esprimersi in maniera consona ed adeguata all'ambiente di apprendimento;
- rispettare il turno di parola;
- utilizzare un linguaggio corretto e rispettoso;
- non aggiungere e/o togliere persone durante la partecipazione alla videoconferenza;
- non diffondere il link e/o il codice e/o il nickname della videoconferenza ad altri;
- non riutilizzare l'invito alla videoconferenza aperta dal docente, dopo il termine della stessa;
- non disturbare, in qualsiasi modo, gli altri partecipanti;
- utilizzare la chat esclusivamente per fini didattici;
- non riprendere quanto compare sullo schermo (foto, video, acquisizione schermo) e/o registrare l'audio durante le videoconferenze, se non dopo avere informato gli altri partecipanti della necessità delle suddette operazioni per ausilio alla memoria e allo studio;
- non diffondere in alcun modo foto o registrazioni relative alle persone presenti in videoconferenza;
- presentarsi alla video-lezione provvisti del materiale necessario per lo svolgimento dell'attività: libro di testo, quaderni o quanto richiesto precedentemente dal docente;
- mostrarsi in video, quando richiesto;
- non consentire ad altri (anche componenti della famiglia) la presenza alle video-lezioni.

Netiquette

La **Netiquette**, parola derivata dalla contrazione del vocabolo inglese *net* (rete) e quello di lingua francese *étiquette* (buona educazione), è un insieme di regole che disciplinano il comportamento di un utente di Internet nel comunicare con altri utenti.
Il rispetto della netiquette non è imposto da alcuna legge, ma si rende necessario, in primo luogo, per le caratteristiche della comunicazione on-line, costretta a fare i conti con:

- la **mancanza di** quelle **informazioni accessorie** (tono della voce, postura, espressione del viso, ecc.) che, nella comunicazione *vis-à-vis*, ci aiuta a comprendere meglio il messaggio e le intenzioni del nostro interlocutore;
- la necessità di rendere gli utilizzatori della Rete consapevoli delle loro **responsabilità nella modalità di accesso e di trasmissione delle informazioni** attraverso Internet.

Di seguito, le regole di buona educazione digitale per una serie di strumenti utilizzati in Istituto:

Chat e Forum

in Chat e Forum inviare messaggi brevi che descrivano in modo chiaro l'oggetto della comunicazione; indicare sempre chiaramente l'oggetto in modo tale che il destinatario possa immediatamente individuare l'argomento.

Scrittura di una mail: DESTINATARI

Gli indirizzi dei destinatari possono essere inseriti in tre campi diversi:

A: qui si inserisce l'indirizzo del destinatario principale dell'email

CC:qui si inserisce l'indirizzo di persone interessate a conoscere il contenuto dell'email. È l'equivalente del "per conoscenza". Quando si riceve un'email in copia non si è tenuti a rispondere se non esplicitamente chiamati in causa.

CCN: tutti gli indirizzi inseriti in questo campo sono visibili solo a chi manda e riceve le email. Quando si inviano email a un numero nutrito di persone è sempre consigliabile inserire gli indirizzi in questo campo, non solo per motivi di privacy, ma anche per evitare che vengano "rubati" in caso di violazione di qualcuno degli account dei destinatari.

Scrittura di una mail: OGGETTO

È forse l'elemento più importante dell'email, sia perché ci aiuta subito a capire il contenuto del messaggio (e la sua importanza) sia perché ci aiuta in eventuali ricerche successive. Questo è il motivo per cui **va sempre inserito**. Se si utilizza la funzione "Rispondi" per scrivere una nuova email, bisogna quindi **cambiare il contenuto dell'oggetto** e cancellare la parte del vecchio messaggio che si troverà in calce all'email. Per questo **è sconsigliato usare la funzione RISPONDI** per scrivere una nuova email.

Scrittura di una mail: CORPO (CONTENUTO)

Sinteticità e chiarezza sono gli elementi che dovrebbero guidare nella stesura del testo. Il numero di email che riceviamo giornalmente è elevato e questo agevola la risposta del nostro interlocutore. Se scriviamo con un indirizzo mail che non permette di riconoscere l'autore del messaggio (come nel caso di indirizzi "fantasiosi" o istituzionali, come quello ufficiale della scuola) **occorre firmarsi**. Ricordarsi sempre che in Rete **SCRIVERE TUTTO MAIUSCOLO EQUIVALE A URLARE,** dunque è fortemente deprecato.

Scrittura di una mail: RISPONDI

Se i destinatari dell'email a cui dobbiamo rispondere sono più d'uno, occorre **decidere se rispondere solo all'autore dell'email o se rispondere a tutti**. Questo ovviamente dipende dal contenuto e dallo scopo della risposta. Il principio da seguire è quello di riempire la casella di posta solo di chi è interessato a quella email.

Scrittura di una mail: ALLEGATI

Gli allegati non dovrebbero essere troppo "pesanti", come per esempio quando si devono spedire molte immagini. Fortemente raccomandato è **attribuire nomi comprensibili ai file**, soprattutto se sono più di uno. E' opportuno fare riferimento agli allegati nel corpo della mail.

Prevenzione, rilevazione e gestione dei rischi legati all'utilizzo di Internet

Prevenzione

La scuola si impegna ad attrezzare le aule con dispositivi elettronici sicuri e protetti.
I docenti si impegnano ad organizzare per gli alunni momenti di riflessione sui temi dell'utilizzo consapevole di internet e a formarsi su queste tematiche.
I genitori si impegnano a prendere visione della E-Safety Policy e a seguire le azioni promosse dalla scuola per l'utilizzo consapevole della rete.
Gli alunni si impegnano a rispettare i regolamenti e a partecipare attivamente alle occasioni di confronto su queste tematiche organizzate dalla scuola.
Per i rischi connessi all'utilizzo delle nuove tecnologie (grooming, cyberbullismo, furto di identità, sexting), la scuola si affida a consulenti esterni per organizzare incontri informativi rivolti agli alunni.

Rilevazione

Si considerano da segnalare tutte quelle situazioni che si configurano come episodi di cyberbullismo (caratterizzate da *volontarie e ripetute aggressioni* mirate a insultare, minacciare, diffamare e/o ferire una persona o un piccolo gruppo tramite un utilizzo irresponsabile dei social network), ma anche usi inappropriati della rete (siti d'odio, contenuti non adatti all'età degli alunni…).
I docenti di classe informano il referente per il Cyberbullismo, il Dirigente o lo staff di Presidenza. Il Dirigente Scolastico procede ad informare le famiglie. Tutte le segnalazioni riportate dai docenti vengono registrate su apposita scheda ed inserite nel registro dei coordinatori di classe.
É in ogni caso necessario, nelle fasi di rilevazione e gestione degli episodi qualificabili come adescamento, cyberbullismo, sexting e altri atti lesivi tipicamente legati all'utilizzo delle tecnologie dell'informazione e della comunicazione con particolare riguardo ai social networks, individuare e adottare misure e procedure per tutelare la riservatezza degli studenti comunque coinvolti, circoscrivendo alle figure e ai ruoli strettamente necessari la comunicazione e la gestione dell'identità degli studenti e dello svolgimento dei fatti.
A tal proposito la scuola ha adottato un'estensione del patto di corresponsabilità (visibile a questo link).

Gestione dei casi

Per un'efficace gestione dei rischi più comuni, ci si attiene alle modalità illustrate nello schema (in allegato) messo a disposizione dal progetto "Generazioni Connesse", di cui in premessa.

Rapallo, 27 maggio 2025