E-Safety Policy

INDICE

1. Introduzione

Scopo della Policy.

Lo scopo della E-Safety Policy è di stabilire i principi fondamentali da fare osservare a tutti i membri della comunità scolastica per quanto riguarda l'utilizzo di tecnologie; salvaguardare e proteggere i bambini, i ragazzi e lo staff dell'Istituto; assistere il personale della scuola a lavorare in modo sicuro e responsabile con altre tecnologie di comunicazione di Internet e monitorare i propri standard e le prassi; impostare chiare aspettative di comportamento e/o codici di condotta rilevanti per un uso responsabile di Internet a scopo didattico, personale o ricreativo; affrontare gli abusi online come il Cyberbullimo, che sono riferimenti incrociati con le altre politiche della scuola; garantire che tutti i membri della comunità scolastica siano consapevoli del fatto che il comportamento illecito o pericoloso è inaccettabile e che saranno intraprese le opportune azioni disciplinari e giudiziarie.

Le principali aree di rischio per la nostra comunità scolastica possono essere riassunte come segue:

Contenuto

l'esposizione a contenuti inappropriati;
visita di siti web inappropriati;
siti di odio;
validazione dei contenuti: come controllare l'autenticità e l'esattezza dei contenuti online.

Contatto

grooming-adescamento;
bullismo on-line in tutte le forme;
il furto di identità.

Condotta

questioni di privacy, tra cui la divulgazione di informazioni personali;
reputazione online;
la salute e il benessere (quantità di tempo speso online su Internet o giochi);
sexting (invio e ricezione di immagini personali intime);
Copyright (poca cura o considerazione per i diritti d'autore relativamente a musica e film).

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

Il Dirigente Scolastico

- la responsabilità generale per i dati e la sicurezza dei dati;
- garantire che la scuola utilizzi un Internet Service filtrato approvato, conforme ai requisiti di legge vigenti;
- la responsabilità di assicurare che il personale riceva una formazione adeguata per svolgere i ruoli di sicurezza on-line e per la formazione di altri colleghi;
- essere a conoscenza delle procedure da seguire in caso di infrazione della E-Safety Policy;
- ruolo di primo piano nello stabilire e rivedere la E-Safety Policy;
- ricevere relazioni di monitoraggio periodiche della sicurezza online da parte del responsabile;
- garantire che vi sia un sistema in grado di monitorare il personale di supporto che svolge le procedure di sicurezza online interne.

I responsabili della sicurezza online (docente su nomina del DS)

- la responsabilità per i problemi di sicurezza online;
- promuovere la consapevolezza e l'impegno per la salvaguardia online in tutta la comunità scolastica;
- assicurare che l'educazione alla sicurezza online sia incorporata in tutto il programma di studi;
- garantire che tutto il personale sia a conoscenza delle procedure che devono essere seguite in caso di incidente per la sicurezza online;
- facilitare la formazione e la consulenza per tutto il personale;
- coordinare con le autorità locali e le agenzie competenti;
- controllare la condivisione di dati personali;
- controllare l'accesso a materiali illegali/inadeguati;
- controllare probabili azioni di cyberbullismo .

L' Animatore Digitale ed il suo team

- pubblicare la E-Safety Policy sul sito della scuola;
- diffusione della E- Safety Policy attraverso mezzi adeguati;
- garantire che tutti i dati relativi agli alunni pubblicati sul sito siano sufficientemente tutelati.

Gli insegnanti

- supervisionare e guidare gli alunni con cura quando sono impegnati in attività di apprendimento che coinvolgono la tecnologia on-line;
- garantire che gli alunni siano pienamente consapevoli delle capacità di ricerca e siano pienamente consapevoli dei problemi legali relativi ai contenuti elettronici come ad esempio le leggi sul copyright.

Il **personale scolastico**

- comprendere e contribuire a promuovere politiche di e-sicurezza ;
- essere consapevoli dei problemi di sicurezza on-line connessi con l'uso di telefoni cellulari, fotocamere e dispositivi portatili;
- monitorare l'uso di dispositivi tecnologici e attuare politiche scolastiche per quanto riguarda questi dispositivi;
- segnalare qualsiasi abuso sospetto o problema ai responsabili della sicurezza online;
- usare comportamenti sicuri, responsabili e professionali nel l'uso della tecnologia;
- garantire che le comunicazioni digitali con gli studenti dovrebbero essere a livello professionale e solo attraverso i sistemi scolastici, non attraverso meccanismi personali, per esempio mail, telefoni cellulari, ecc.

Gli alunni

- leggere, comprendere, ed accettare la E- Safety Policy ;
- avere una buona comprensione delle capacità di ricerca e la necessità di evitare il plagio e rispettare normative sul diritto d'autore;
- capire l'importanza di segnalare abusi, o l' uso improprio o l'accesso a materiali inappropriati;
- sapere quali azioni intraprendere se loro oqualcuno che conoscono si sente preoccupato o vulnerabile quando si utilizza la tecnologia on-line;
- conoscere e capire la politica relativa all'uso dei telefoni cellulari, fotocamere digitali e dispositivi portatili;
- conoscere e capire la politica della scuola sull' uso di immagini e il cyberbullismo;
- capire l'importanza di adottare buone pratiche di sicurezza on-line quando si usano le tecnologie digitali fuori dalla scuola;
- assumersi la responsabilità di conoscere i benefici e i rischi di utilizzo di Internet e di altre tecnologie in modo sicuro, sia a scuola che a casa.

I **genitori**

- sostenere la scuola nel promuovere la sicurezza online e approvare l'accordo di E-Safety Policy con la scuola;
- leggere, comprendere e controfirmare il suddetto accordo;
- accedere al sito web della scuola in conformità con quanto stabilito dalla stessa;
- assicurarsi che la scuola abbia preso tutte le precauzioni necessarie circa un uso corretto della tecnologia da parte degli alunni.

Al fine di garantire una gestione il più possibile corretta, la scuola attua le seguenti strategie:

Il Dirigente Scolastico si riserva, sentiti i responsabili, di limitare l'accesso e l' uso della rete interna

{Intranet) ed esterna {Internet) secondo i normali canali di protezione presenti nei sistemi operativi.

Si attrezza per evitare comportamenti che non rientrano nelle norme che il Collegio dei Docenti delinea in proposito, come:

- scaricare file video-musicali protetti da copyright;
- visitare siti non necessari ad una normale attività didattica;
- alterare i parametri di protezione dei computer in uso;
- utilizzare la rete per interessi privati e personali che esulano dalla didattica;
- non rispettare le leggi sui diritti d'autore;
- navigare su siti non accettati dalla protezione interna alla scuola.

Disposizioni, comportamenti, procedure:

- Il sistema informatico è periodicamente controllato dai responsabili (docente responsabile su nomina del Dirigente Scolastico).
- La scuola può controllare periodicamente i file utilizzati, i file temporanei e i siti visitati da ogni macchina.
- La scuola archivia i tracciati del traffico Internet.
- E' vietato installare e scaricare da Internet software non autorizzati.
- Le postazioni PC in ambiente Windows sono protette da software che impediscono modifiche ai dati memorizzati sul disco fisso interno.
- Al termine di ogni collegamento la connessione deve essere chiusa.
- Verifiche antivirus sono condotte periodicamente sui computer e sulle unità di memorizzazione di rete.
- L'utilizzo di CD, chiavi USB e floppy personali deve essere autorizzato dal docente e solo previa scansione antivirus per evitare qualsiasi tipo di infezione alla rete d'Istituto.
- La scuola si riserva di limitare il numero di siti visitabili e le operazioni di download.
- Il materiale didattico dei docenti può essere messo in rete, anche su siti personali collegati all'Istituto, sempre nell'ambito del presente regolamento e nel rispetto delle leggi.

Condivisione e comunicazione della Policy all'intera comunità scolastica.

La E-Safety 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.

Il Dirigente Scolastico regola il comportamento degli studenti e autorizza i membri del personale di imporre sanzioni disciplinari per il comportamento inadeguato. Questo è pertinente a episodi di cyberbullismo, o altri tipi di incidenti che possono danneggiare la sicurezza online.

La scuola si occuperà di tali incidenti all'interno di questa Policy, delle politiche di comportamento e anti- bullismo associati ed avrà il compito di informare i genitori di episodi di comportamento inappropriato di sicurezza online, che si svolgono all'interno della scuola.

La Policy sarà comunicata al personale, agli alunni, alla comunità nei seguenti modi:

- pubblicazione della E-Safety Policy sul sito della scuola;
- accordo di utilizzo accettabile, discusso 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;
- accordo di utilizzo accettabile rilasciato al personale scolastico.

Gestione delle infrazioni alla Policy:

La scuola prenderà tutte le precauzioni necessarie per garantire la sicurezza on-line. Tuttavia, a causa della scala internazionale collegata ai contenuti Internet, la disponibilità di tecnologie mobili e velocità di cambiamento, non è possibile garantire che il materiale non idoneo apparirà mai su un computer della scuola o dispositivo mobile. Né la scuola né l'autorità locale possono accettare la responsabilità per il materiale accessibile, o le conseguenze di accesso a Internet.
Al personale e agli alunni saranno date informazioni sulle infrazioni in uso e le eventuali sanzioni. Le suddette sanzioni includono:

informare il docente della classe, il docente responsabile della sicurezza online o il Dirigente Scolastico;

informare i genitori o i tutori;

il ritiro del cellulare fino a fine giornata;

la rimozione di Internet o del computer di accesso per un periodo:

la comunicazioni alle autorità competenti.

Il docente responsabile della sicurezza online fungerà da primo punto di contatto per qualsiasi reclamo. Qualsiasi lamentela personale di abuso sarà riferita al Dirigente Scolastico.

Denunce di bullismo online saranno trattate in conformità con la legge attuale. Reclami relativi alla protezione dei bambini saranno trattati in conformità alle procedure di protezione dell'infanzia.

Monitoraggio dell'implementazione della Policy e suo aggiornamento

La E-Safety Policy si inserisce all'interno di altre politiche scolastiche, quali la politica di protezione dei minori, la politica anti-bullismo, la politica del benessere degli alunni a scuola.
La scuola avrà un docente responsabile della sicurezza online che sarà si prenderà cura della revisione e/o aggiornamento della Policy sotto la super visione del DS.

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 discusse in dettaglio con tutti i membri del personale docente.

Nell'ambito della revisione della Policy, tutte le informazioni e le revisioni saranno memorizzate per eventuali controlli, sulla base del seguente documento:

Versione	1.0
Data	**GG/MM/AAAA**
Autore	Nome del docente responsabile della sicurezza online (E-Safety Policy)
Approvato dal Dirigente	
Approvato dal Collegio docenti	
Prossima data di revisione	

Modifica

Versione	Data	Descrizione	Nome del docente responsabile della sicurezza online (E-Safety Policy)
0.1			

Nell'ambito del monitoraggio dell'implementazione della E-Safety Policy si terranno in considerazione i dati annuali sulla base del seguente documento:

a.s...../.....	Numero di Segnalazioni	Numero di Infrazioni	Numero di Sanzioni Disciplinari

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, con valenza pluriennale, è quindi un'opportunità per innovare la Scuola, adeguando non solo le strutture e le dotazioni tecnologiche a disposizione dei docenti e dell'organizzazione, ma soprattutto le metodologie didattiche e le strategie usate con gli alunni in classe.

L'**O.M. 851 del 27 ottobre 2015,** in attuazione dell' art .1, comma 56 della legge 107/2015, ne ha previsto l'attuazione al fine di:

- migliorare le competenze digitali degli studenti anche attraverso un uso consapevole delle stesse;
- implementare le dotazioni tecnologiche della scuola al fine di migliorare gli strumenti didattici e laboratoriali ivi presenti;
- favorire la formazione dei docenti sull'uso delle nuove tecnologie ai fini dell'innovazione didattica;
- individuare un Animatore Digitale ed un team per l'innovazione digitale che supporti ed accompagni adeguatamente l'innovazione didattica, nonché l'attività dell'animatore Digitale;
- partecipare a bandi nazionali ed europei per finanziare le suddette iniziative;

Curricolo sulle competenze digitali per gli studenti

Nell'ambito del PNSD questa scuola si propone un programma di progressiva educazione alla sicurezza, online come parte del curriculum scolastico. Si impegna a sviluppare una serie di competenze e comportamenti adeguati alle età degli alunni e ad esperienza, tra cui:

- programmare attività e far partecipare gli alunni a laboratori di Coding in occasione della Settimana del codice;
- sviluppare una serie di strategie per valutare e verificare le informazioni prima di accettare l'esattezza;
- essere a conoscenza che l'autore di un sito web/ pagina può avere un particolare pregiudizio;
- sapere come restringere o affinare una ricerca;
- capire il comportamento accettabile quando si utilizza un ambiente online, vale a dire , essere educato, non utilizzare comportamenti inappropriati, mantenere le informazioni personali private;
- capire come le fotografie possono essere manipolate e individuare contenuti web in grado di attrarre il tipo sbagliato di attenzione;
- capire perché 'amici' on-line potrebbero non essere chi dicono di essere e di comprendere perché dovrebbero fare attenzione in 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;
- sapere di non scaricare alcun file - come i file musicali - senza permesso;
- comprendere l'impatto di bullismo online, sexting, grooming e sapere come cercare aiuto se sono in pericolo;
- sapere come segnalare eventuali abusi tra cui il bullismo on-line e come a chiedere aiuto ai docenti, ai genitori, se si verificano problemi quando si utilizzano le tecnologie Internet;
- utilizzare con attenzione Internet per garantire che si adatti alla loro età e supporti gli obiettivi di apprendimento per le aree curriculari specifiche.

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

Nell'ambito del PNSD questa scuola ha previsto:

- individuazione e formazione di un Animatore Digitale e del Team per l' attuazione degli obiettivi e delle innovazioni previste dal PSND;
- formazione dei docenti all' utilizzo del registro elettronico e dello scrutinio elettronico;
- somministra zione di un questionario rivolto ai docenti per la rivelazione dei bisogni " digitali ";
- realizzazione / ampliamento della rete WI-FI/ LAN dei tre plessi dell' Istituto ;
- ricognizione e messa a punto delle dotazioni digitali ;
- attivazione e comunicazione di iniziative di formazione, in particolare rivolte allo sviluppo e alla diffusione del Coding e del pensiero computazionale;
- monitoraggio del piano digitale di Istituto e dei risultati conseguiti;
- si assicura che il personale sa come inviare o ricevere dati sensibili o personali e comprendere l'obbligo di crittografare i dati dove la sensibilità richiede protezione degli stessi;
- offre una formazione a disposizione del personale in materia di sicurezza on-line attraverso corsi di formazione e/o aggiornamento;
- fornisce, come parte del processo di induzione, tutto il nuovo personale con informazioni e indicazioni sulla E-Safety Policy d'Istituto.

Sensibilizzazione delle famiglie.

Questa scuola esegue un programma continuativo di consulenza, orientamento e formazione per i genitori, tra cui:

- presentare ai genitori, i cui figli si scrivono nel nostro Istituto, il Regolamento della Policy, al fine di garantire che i principi di comportamento sicuro on-line siano chiari;
- distribuire volantini di informazione e pubblicazioni sul sito della scuola;
- offrire incontri di consulenza con esperti;
- fornire informazioni sui siti nazionali di sostegno per i genitori, quali il sito www.generazioniconnesse.it.

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

E-mail

Questa scuola non pubblica indirizzi di posta elettronica personali degli alunni o del personale sul sito della scuola.

Sarà contattato il Dirigente Scolastico se qualcuno dello staff o degli alunni riceve una e-mail che consideriamo particolarmente preoccupante o che infrange la legge.

Farà rapporto di attività illegali alle competenti autorità e, se necessario, alla polizia.

Sa che spam, phishing e virus allegati possono rendere le mail pericolose. Perciò si utilizzeranno una serie di tecnologie per proteggere utenti e sistemi nella scuola, tra cui Anti-Virus, oltre al filtraggio delle email.

Sito web della scuola

L'Istituto dispone di un proprio spazio web e di un proprio dominio: www.icsviadavinci.it.

L'Istituto gestisce un proprio sito web nello spazio di proprietà. La gestione del sito della scuola e la rispondenza alle normative per quanto concerne i contenuti (accuratezza, appropriatezza, aggiornamento) e le tecniche di realizzazione e progettazione è a cura del Webmaster. La scuola detiene i diritti d'autore dei documenti che si trovano sul proprio sito o di quei documenti per i quali è stato chiesto ed ottenuto il permesso dall'autore proprietario. Le informazioni pubblicate sul sito della scuola relative alle persone da contattare rispetteranno le norme vigenti sulla privacy.

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.

Sicurezza Rete Lan

L'Istituto dispone di un dominio su rete locale (rete segreteria) cui accedono i computer dell'amministrazione, tali postazioni sono su una rete locale isolata dal resto della rete di Istituto (rete didattica). Il collegamento di computer portatili o palmari personali alla rete di Istituto deve essere autorizzato dal Dirigente Scolastico.

La rete interna è protetta da Firewall per quanto riguarda le connessioni con l'esterno. Le postazioni sono protette con sistemi antivirus regolarmente aggiornati.

La memorizzazione dei documenti e delle impostazioni personali è garantita attraverso il meccanismo di profilo mobili di Windows, che archivia centralmente sul server di dominio i dati, e li rende disponibili in tutte le postazioni legate alla didattica (laboratori, sale insegnanti, postazioni per studenti e docenti). Su questi dispositivi non è garantito alcun servizio di backup, pertanto si consiglia di fare copia su un supporto personale (Pendrive, Hard Disk esterni, o altro) dei propri dati.

Per quanto concerne la rete amministrativa, lo storage è garantito da backup automatico su altra postazione.

Sicurezza della rete senza fili (Wireless - WiFi)

L'Istituto dispone di una rete con tecnologia senza fili. L'accesso alla rete wireless è regolato da un controller che determina l'accesso degli utenti, docenti e studenti, tramite il riconoscimento del dispositivo utilizzato.

L'ottenimento delle credenziali è riservato a studenti e personale dell'Istituto e ospiti. Le regole di comportamento sono analoghe a quelle per la connessione alle reti cablate di Istituto.

4.Strumentazione personale

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

Gli studenti possono utilizzare smartphone, tablet e PC durante le attività didattiche, se non nei casi contemplati nel Patto BYOD, né possono accedere alla rete attraverso i dispositivi della scuola se non dietro previa autorizzazione dell'insegnante presente in aula e comunque per ricerche attinenti le attività didattiche.Gli smartphone, se non utilizzati, vanno riposti in classe in un luogo ben custodito.

Per i docenti: gestione degli strumenti personali - cellulari, tablet ecc..

I docenti possono utilizzare i propri devices, connessi ad internet, per accedere al registro elettronico e per supportare le proprie attività didattiche. Ne è vietato l'utilizzo a fini personali durante l'attività lavorativa.

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

Il personale della scuola può utilizzare cellulari, tablet e PC durante l'orario scolastico soltanto per attività afferenti alle proprie mansioni. Ne è vietato l'utilizzo a fini personali durante l'attività lavorativa.

5. Prevenzione, rilevazione e gestione dei casi

Prevenzione

Principi generali:

Internet favorisce la libertà d'espressione e, quando si entra a far parte di una community o di un servizio dove interagiscono più utenti, vanno considerati abusi meritevoli di segnalazione solo i contenuti palesemente impropri o illeciti e non tutti quei contenuti con cui semplicemente non si è d'accordo o non piacciono.

Quando si inizia a navigare tra i servizi dei Social Network e le applicazioni web tipo YouTube, Facebook, Netlog, etc., 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.

Se si condividono informazioni personali, bisogna farlo scegliendo 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.

Se si condividono elementi multimediali o informazioni che riguardano più persone è necessario avere il permesso di ciascun utente coinvolto prima di effettuare la pubblicazione. Non bisogna pubblicare sul Web video girati di nascosto e dove sono presenti persone filmate senza il loro consenso.

Bisogna contribuire a rendere il Web un luogo sicuro, pertanto ogni volta che un utente commette involontariamente un abuso o un errore, pubblicando del materiale illecito, non idoneo o offensivo, bisogna contattarlo e fornire le spiegazioni relative alle regole, diffondendo così i principi della sicurezza .

Ogni abuso subito o rilevato nella navigazione, deve essere segnalato tramite i canali e gli strumenti offerti dal servizio, indicando in modo semplice i riferimenti per ottenere tempestivamente la rimozione del contenuto (abuso, data, ora, utenti e servizio coinvolti). Tutti i social-network garantiscono la possibilità di segnalare materiale inopportuno mediante semplici operazioni da compiere direttamente sul sito. Prima di trasformare un incidente o una " bravata" in una denuncia alle autorità competenti avvalersi della modalità di segnalazione che non obbliga le parti in causa a conseguenze penali e giudiziarie che possono durare anni.

Scuola e Famiglia possono essere determinanti nella diffusione di un atteggiamento mentale e culturale che consideri la diversità come una ricchezza e che educhi all'accettazione, alla consapevolezza dell' altro, al senso della comunità e della responsabilità collettiva. Occorre, pertanto, rafforzare e valorizzare il Patto di Corresponsabilità

educativa previsto dallo Statuto delle studentesse e degli studenti della Scuola Secondaria: la scuola é chiamata ad adottare misure atte a prevenire e contrastare ogni forma di violenza e di prevaricazione; la famiglia é chiamata a collaborare, non solo educando i propri figli ma anche vigilando sui loro comportamenti.

Per definire una strategia ottimale di prevenzione e di contrasto , le esperienze acquisite e le conoscenze prodotte vanno contestualizzate alla luce dei cambiamenti, che hanno profondamente modificato la società, sul piano etico, sociale e culturale e ciò comporta una valutazione ponderata delle procedure adottate per riadattarle in ragione di nuove variabili, assicurandone in tal modo l' efficacia.

La forma online del bullismo ha però alcune caratteristiche peculiari che lo rendono pericoloso perché:

il cyberbullismo è pervasivo: il cyberbullo può raggiungere la sua vittima in qualsiasi momento e in qualsiasi luogo. La possibilità di avere smartphone sempre accesi e spesso connessi ad internet permette al cyberbullo di aggredire la sua vittima ogni volta che lo desidera;

è un fenomeno persistente: il materiale diffamatorio pubblicato su internet può rimanere disponibile online anche per molto tempo;

spettatori e cyberbulli sono potenzialmente infiniti: le persone che possono assistere ad episodi di cyberbullismo sono potenzialmente illimitate e molti possono essere cyberbulli, anche solo condividendo o promuovendo l'episodio di cyberbullismo, che finisce per replicarsi (ad esempio sulle bacheche dei profili che i ragazzi hanno sui socia! network) in modo incontrollabile.

La scuola si impegna a:

riconoscere il Dirigente Scolastico come titolare del trattamento di dati personali secondo la Legge sulla privacy (art. 41 f del D.Lgs. 196/ 2003);

riconoscere come responsabile della sicurezza online un docente su nomina del Dirigente Scolastico;

nominare l' Animatore Digitale ed il team che lo affiancherà, su nomina del Dirigente Scolastico dopo richiesta di disponibilità fatta con circolare.

La Scuola si impegna inoltre ad organizzare le seguenti attività di prevenzione al fenomeno:

organizzazione di Corsi di formazione per docenti, genitori, operatori del settore socio-educativo;

monitoraggio sul tema del cyberbullismo attraverso questionari (Allegato n.3);

partecipazione da parte di docenti, studenti e genitori a convegni e seminari sul tema del bullismo e del cyberbullismo;

interventi di consulenza e supporto - su richiesta da parte della scuola - relativamente a casi di cyberbullismo.

I docenti si impegnano a :

accompagnare gli alunni nella navigazione in Rete, coinvolgendoli nell'esplorazione delle opportunità e dei rischi, con attività calendarizzate dall'inizio dell'anno;

approfondire, con attività mirate in classe, la conoscenza del fenomeno del bullismo e del cyber bullismo;

creare degli spazi in cui gli alunni si possano confrontare su questo tema, utilizzando come spunti di riflessione: spezzoni di film, canzoni, materiali prodotti da altri alunni coinvolti nel progetto SIC;

mantenere viva una task-force interna all'istituto, che possa progettare attività formative sul fenomeno del cyberbullismo e calendarizzarle per tutta la comunità scolastica;

confrontarsi con gli altri insegnanti della classe, della scuola o con esperti del territorio;

rivolgersi alla helpline di generazioni connesse (www.generazioniconnesse.it).

I genitori si impegnano a :

firmare il patto di Corresponsabilità redatto dalla scuola;

prendere visione della E-Safety Policy messa a disposizione di docenti, genitori ed alunni sul sito della scuola www.icsviadavinci.it;

seguire le azioni promosse dalla scuola per un uso corretto della rete;

frequentare corsi di formazione/convegni che la scuola organizzerà per la diffusione di informazioni legate ad un uso corretto della tecnologia digitale.

Gli alunni si impegnano a:

prendere visione del Patto di Corresponsabilità che i genitori hanno firmato con la scuola;

prendere visione della E-Safety Policy pubblicata sul sito web della scuola;

rispettare le regole per un uso corretto della tecnologia;

denunciare qualsiasi caso di abuso online;

prendere parte a qualsiasi evento che la scuola organizza in materia di sicurezza online.

Rilevazione e gestione dei casi

Intervenire in situazioni di cyberbullismo non è mai semplice: spesso si pensa di non sapere esattamente cosa fare e si ha timore di essere inadeguati. Per tale motivo la scuola si impegna ad individuare due strumenti che potranno agevolare l'intera comunità scolastica:

nel decidere come intervenire;

nel tenere traccia di ciò che è avvenuto rispetto ai comportamenti degli alunni online e di come è stato gestito il problema.

L'obiettivo a lungo termine, che come comunità scolastica ci diamo, è quello di creare una memoria condivisa non solo di ciò che accade nella scuola rispetto al web, ma anche di strutturare una fonte esemplificativa che possa orientare sempre più e sempre meglio le azioni di contrasto ad episodi che, nel tempo, potrebbero ripetersi.

Per una efficace gestione dei casi la scuola si riserva di utilizzare lo schema messo a disposizione sul sito www.generazioniconnesse.it (Allegato n.1).

Per poter tenere traccia di ciò che è avvenuto rispetto ai comportamenti degli alunni online e di come è stato gestito il problema, la scuola si riserva di utilizzare il "Diario di Bordo" messo a disposizione sul sito www.generazioniconnesse.it (Allegato n.2).

Annessi (da prodursi a cura della scuola)

Procedure operative per la protezione dei dati personali.

Informativa ex artt.. 13 e 14 del regolamento UE 2016/679 per il trattamento dei dati personali di alunni e familiari.

Procedure operative per la rilevazione, il monitoraggio e la gestione delle segnalazioni.
(Allegato n. 1; Allegato n.2; Allegato n.3).

Procedure operative per la gestione delle infrazioni alla Policy (Allegato n.4).

Protocolli siglati con le forze dell'ordine e i servizi del territorio per la gestione condivisa dei casi.
Non vi sono protocolli siglati ma ricorrenti forme di collaborazione nella prevenzione e contrasto del bullismo e del Cyberbullimo.

Allegati:

Allegato 5 Documento di E-Safety Policy: Consenso dei Genitori/Tutori per l'accesso ad Internet e Dichiarazione liberatoria per la pubblicazione di elaborati, nomi, voci, immagini, materiale audiovisivo sul sito della scuola.

Allegato 6 Documento di E-Safety Policy: Assunzione di responsabilità da parte degli Studenti per l'uso consapevole di Internet.

Allegato 7 Documento di E-Safety Policy: Assunzione di responsabilità da parte di Docenti e altro Personale della Scuola.

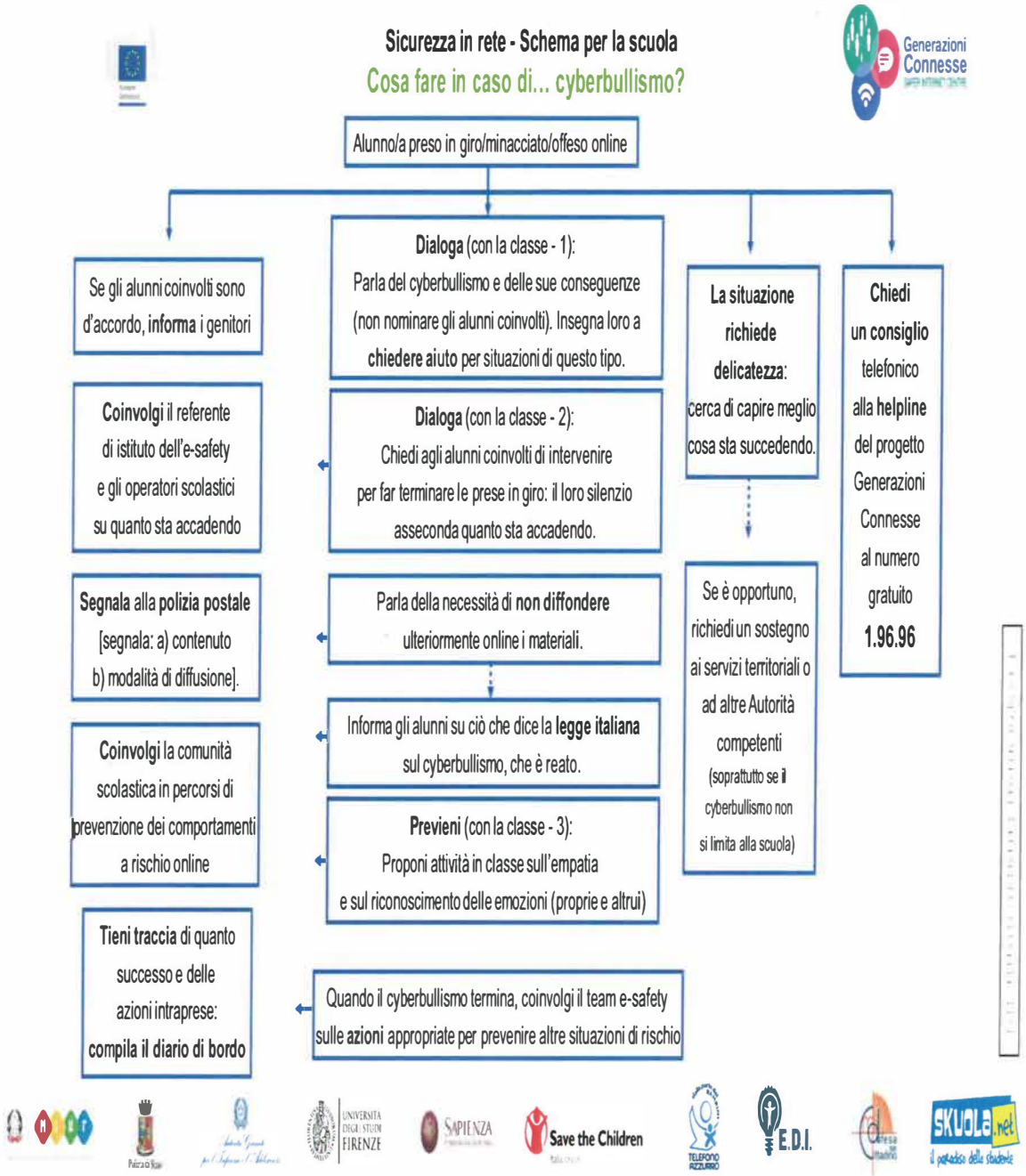
Allegato 8 Patto BYOD A1.

Allegato 8bis Patto BYOD A2 .

Il referente
Prof. Maurizio MUZZI

Il D ri ente Scolastico
Dott.ssa Tiziana Aloisi

ALLEGATO N.1


Sicurezza in rete - Schema per la scuola
Cosa fare in caso di... cyberbullismo?
Generazioni Connesse
Alunno/a preso in giro/minacciato/offeso online
Se gli alunni coinvolti sono d'accordo, informa i genitori
Dialoga (con la classe - 1): Parla del cyberbullismo e delle sue conseguenze (non nominare gli alunni coinvolti). Insegna loro a chiedere aiuto per situazioni di questo tipo.
La situazione richiede delicatezza: cerca di capire meglio cosa sta succedendo.
Chiedi un consiglio telefonico alla helpline del progetto Generazioni Connesse al numero gratuito 1.96.96
Coinvolgi il referente di istituto dell'e-safety e gli operatori scolastici su quanto sta accadendo
Dialoga (con la classe - 2): Chiedi agli alunni coinvolti di intervenire per far terminare le prese in giro: il loro silenzio asseconda quanto sta accadendo.
Se è opportuno, richiedi un sostegno ai servizi territoriali o ad altre Autorità competenti (soprattutto se il cyberbullismo non si limita alla scuola)
Segnala alla polizia postale [segnala: a) contenuto b) modalità di diffusione].
Parla della necessità di non diffondere ulteriormente online i materiali.
Coinvolgi la comunità scolastica in percorsi di prevenzione dei comportamenti a rischio online
Informa gli alunni su ciò che dice la legge italiana sul cyberbullismo, che è reato.
Previeni (con la classe - 3): Proponi attività in classe sull'empatia e sul riconoscimento delle emozioni (proprie e altrui)
Tieni traccia di quanto successo e delle azioni intraprese: compila il diario di bordo
Quando il cyberbullismo termina, coinvolgi il team e-safety sulle azioni appropriate per prevenire altre situazioni di rischio
Save the Children
E.D.I.
SKUOLA.net

Allegato 2

Sicurezza in rete - Schema per la scuola

Schema riepilogativo delle situazioni gestite legate a rischi online (ALLEGATO N.2)

Riepilogo casi
Scuola_____ Anno Scolastico_____

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

ALLEGATO N.3

QUESTIONARIO

Ti preghiamo di rispondere con sincerità a tutte le domande e di lavorare autonomamente senza commentarle con i compagni. Le tue risposte saranno molto importanti per migliorare la vita dei ragazzi a scuola.

Ti ricordiamo che i questionari non sono un compito scolastico, non esiste una risposta giusta o sbagliata, quella più immediata e spontanea è la migliore!

Le risposte ai questionari sono confidenziali e non sarà mai possibile risalire al tuo nome e che sei libero di rifiutarti di rispondere.

Se vorrai, dopo potremmo discutere del questionario insieme ai tuoi insegnanti. Nessuno a scuola o a casa saprà in che modo hai risposto a queste domande.

Molte domande riguardano la tua vita a scuola dal momento in cui è iniziata, cioè a partire da settembre.

Quando rispondi cerca di pensare a tutto questo periodo e non soltanto agli ultimi giorni o mesi.

Ora puoi procedere.

Ti ringraziamo per la collaborazione.

SESSO M ☐ F ☐

CYBERBULLISMO

Il Cyberbullismo (o bullismo elettronico) è una nuova forma di prepotenza che prevede l'utilizzo di e-mail, messaggi di testo (SMS), chat, siti web, telefoni cellulari o altre forme di informazione tecnologica allo scopo di tormentare, minacciare o intimidire qualcuno diffondere dicerie e storie non vere sul conto di altri. Il Cyberbullismo può includere alcune azioni come minacce, insulti su diversa razza e ripetuta vittimizzazione di qualcuno tramite supporto elettronico.

Conosci qualcuno che ha subito prepotenze attraverso il Cyberbullismo in questo anno scolastico?

☐ No

☐ Sì, fuori dalla scuola

☐ Sì a scuola

☐ Sì, sia a scuola che fuori dalla scuola

Hai mai subito prepotenze attraverso il Cyberbullismo in questo anno scolastico?

☐ No ☐ Sì, dai compagni di scuola

Che tipo di esperienzahai avuto?

	Mai	Solo 1 volta	2-3volteal mese	1voltaa settimana	Diverse volte allasettimana
Mi sono arrivati brutti messaggi di testo SMS (facendo minacce e commenti)					
Foto/video offensivi sul cellulare					
Mi hanno fatto scherzi o telefonate mute					
Attraverso cattive o brutte e-mail					
Hanno diffuso riprese o foto di mie situazioni imbarazzanti o intime su internet o con il telefonino.					
Hanno diffuso dicerie sul mio conto tramite web e/o SMS, MSN, FACEBOOK					
Ho ricevuto insulti sulla rete (MSN Messenger/AOL/Yahoo FACEBOOK					
Altro (scrivi cosa)					

Hai mai preso parte ad episodi di Cyberbullismo in questo anno scolastico?

☐ No

☐ Qualche volta

☐ Spesso

A che tipo di comportamento hai preso parte in questo anno scolastico?

	Mai	Solo 1 volta o 2	2-3volteal mese	1voltaa settimana	Diverse volte allasettimana
Inviare (ho inviato) brutti messaggi di testo SMS (facendo minacce e commenti))					
Foto/video offensivi sul cellulare					
Scherzi o telefonate mute					
Inviare (Ho inviato) cattive o brutte e-mail					
Diffondere riprese o foto di situazioni imbarazzanti o intime su internet o con il telefonino.					
Diffondere dicerie sul conto di altri tramite web e/o SMS, MSN, FACEBOOK					
Insultare sulla rete tramite MSN Messenger/AOL/Yahoo FACEBOOK					
h.Altro(scrivi cosa)					

ALLEGATO N. 4

Procedure operative per la gestione delle infrazioni alla E-Safety Policy.

Ogni volta che un membro del personale o studente viola la E-Safety Policy, la decisione finale sul livello di sanzioni sarà a discrezione del Dirigente Scolastico e rifletterà le procedure comportamentali e disciplinari della scuola.

Di seguito sono fornite solo come esemplificazione:

STUDENTI:

INFRAZIONI	**POSSIBILI SANZIONI**
Uso di siti non-educativi durante le lezioni. Utilizzo non autorizzato di e-mail. Uso non autorizzato del telefono cellulare altre nuove tecnologie) durante le lezioni. Uso di instant messaging / siti di social networking.	Fare riferimento all'insegnante della classe/ docente responsabile della sicurezza online/Dirigente Scolastico
Uso continuato di siti non-educativi durante le lezioni dopo essere stato avvertito. Uso non autorizzato di e-mail dopo essere stato avvertito. Uso non autorizzato del telefono cellulare (o altre nuove tecnologie) dopo essere stato avvertito. Uso continuato messaggistica / chat room istantanea, siti di social networking, newsgroup. Uso di materiale offensivo .	Fare riferimento all'insegnante della classe/ docente responsabile della sicurezza online/Dirigente Scolastico Escalation a: rimozione dei diritti di accesso a Internet per un periodo; rimozione di telefono fino a fine giornata; contatto con i genitori.
Rovinare o distruggere deliberatamente i dati di qualcuno, violare la privacy altrui o messaggi inappropriati, video o immagini su un sito di social networking. Invio di un messaggio e-mail o MSN che è considerato molestia o azione di bullismo. Cercare di accedere a materiale offensivo o pornografico.	Fare riferimento all'insegnante della classe/ docente responsabile della sicurezza online/Dirigente Scolastico Escalation a: rimozione dei diritti di accesso a Internet per un periodo; rimozione di telefono fino a fine giornata; contatto con i genitori. contattare le autorità competenti.
Invio di e-mail o messaggi di MSN considerati molestia o bullismo dopo essere stato avvertito. Accedere deliberatamente allo scaricamento o alla diffusione di qualsiasi materiale ritenuto offensivo, osceno, diffamatorio, razzista, omofobico o violento. Trasmissione di materiale che viola i diritti d'autore di un'altra persona o infranga le condizioni della legge sulla protezione dei dati.	Fare riferimento all'insegnante della classe / contatto con i genitori Altre possibili azioni di salvaguardia: conservare le prove; informare i provider di servizi di posta elettronica del mittente; fare rapporto alle autorità competenti dove si sospetti la pedofilia o altre attività illegali.
Portare il nome della scuola in discredito.	

PERSONALE SCOLASTICO

INFRAZIONI	POSSIBILI SANZIONI
Uso di Internet per attività personali non legate allo sviluppo professionale (shopping online, e-mail personali, instant messaging ecc.). Utilizzo di supporti di memorizzazione dei dati personali (ad esempio, chiavette USB) senza considerare l'accesso e l'adeguatezza di qualsiasi file memorizzato. Non implementare adeguate procedure di salvaguardia. Qualsiasi comportamento sul World Wide Web che compromette la professionalità del personale nella scuola e nella comunità. Uso improprio di primo livello di sicurezza dei dati, ad esempio uso illecito di password. Violazione del copyright o della licenza per l'installazione di software .	Fare riferimento al docente responsabile della sicurezza online /DSGA /Dirigente Scolastico Escalation a: avvertimento
Gravi danni intenzionali all'hardware o software del computer. Qualsiasi tentativo deliberato di violare la protezione dei dati o di sicurezza informatica. Creare, accedere, scaricare e diffondere deliberatamente qualsiasi materiale ritenuto offensivo, osceno, diffamatorio, razzista, omofobico o violento. Ricevere o trasmettere materiale che viola i diritti d'autore di un'altra persona o infranga le condizioni della legge sulla protezione dei dati. Portare il nome della scuola in discredito.	Fare riferimento al docente responsabile della sicurezza online/Dirigente Scolastico Altre azioni di salvaguardia: rimuovere il PC in un luogo sicuro per garantire che non vi è alcun ulteriore accesso al PC o laptop; far verificare tutte le attrezzature per garantire che non vi è alcun rischio di alunni che accedono a materiali inappropriati nella scuola. Escalation a: Contattare e fare rapporto alle autorità competenti

Come saranno informati il personale e gli studenti di queste procedure?

La E-Safety Policy sarà resa disponibile sul sito dell'Istituto a studenti, personale scolastico e genitori.

I genitori firmeranno la E-Safety Policy quando il loro bambino inizierà la scuola.

Agli studenti sarà insegnato un uso responsabile della rete in modo tale che possano sviluppare "comportamenti sicuri".

Informazioni su come segnalare azioni di bullismo o cyber bullismo saranno messe a disposizione dalla scuola per gli alunni, il personale e i genitori.

Allegato5

Documento di E-Safety Policy: Consenso dei Genitori/Tutori per l'accesso ad Internet e Dichiarazione liberatoria per la pubblicazione di elaborati, nomi, voci, immagini, materiale audiovisivo

I sottoscritti ..... e ....., genitori/tutori dell'alunno/a ..... iscritto/a alla classe ..... sez. ..... della scuola dell'infanzia/primaria/secondaria di 1° grado .....

dichiarano

di aver letto e compreso il Documento di E-Safety Policy;

di essere al corrente che la Scuola mette in atto tutte le precauzioni necessarie per garantire al massimo che gli alunni usino correttamente la rete e non accedano a materiale inadeguato;

di essere consapevoli che, in considerazione delle precauzioni prese per ridurre al massimo i rischi della navigazione sul WEB, la Scuola non è responsabile di eventuali usi impropri della rete e delle Tecnologie dell'Informazione e della Comunicazione (TIC) né della natura e dei contenuti del materiale che il/la proprio/a figlio/a, aggirando per volontà propria le barriere predisposte dalla scuola, potrebbero reperire in Internet;

di essere consapevoli della responsabilità individuale del/la proprio/a figlio/a per le eventuali violazioni delle norme e/o per gli eventuali danni provocati da un uso improprio degli strumenti informatici;

di essere consapevoli che, qualora non venissero rispettate le regole, la scuola adotterà sanzioni disciplinari rapportate alla gravità degli episodi e saranno altresì possibili azioni civili per eventuali danni, nonché l'eventuale denuncia all'autorità giudiziaria qualora la violazione si configuri come reato.

Pertanto, i sottoscritti

acconsentono/non acconsentono (barrare la voce che non interessa) che il/la proprio/a figlio/a utilizzi a scuola l'accesso Internet;

autorizzano/non autorizzano (barrare la voce che non interessa) L'Istituto Comprensivo "Da Vinci" a realizzare e ad utilizzare, a scopo didattico e/o di documentazione e/o di informazione e senza fini di lucro, fotografie, video o altri materiali audiovisivi contenenti l'immagine, il nome, la voce, gli elaborati (scritti, disegni, ...) del/la proprio/a figlio/a anche, se del caso, mediante riduzioni e/o adattamenti;

dichiarano di essere informati che detto materiale potrà essere utilizzato per documentare e divulgare le attività della scuola tramite il sito Internet di Istituto, pubblicazioni, CD-ROM, mostre, seminari, convegni e altre iniziative promosse dalla scuola anche in collaborazione con altri soggetti;

dichiarano di non aver nulla a pretendere jn ragione di quanto sopra indicato e di rinunciare irrevocabilmente ad ogni diritto, azione o pretesa derivante da quanto sopra autorizzato.

Allegato:

Fotocopie dei documenti di identità

Firma .....

Firma, ...

Cornaredo.....

Allegato 6

Documento di E-Safety Policy Assunzione di responsabilità da parte degli Studenti per l'uso consapevole di internet

Il/La sottoscritto/a ....., alunno/a della Classe ....., Sez. ..... della scuola secondaria di 1° grado I C "Da Vinci" Cornaredo

dichiara:
di aver letto e compreso il Documento di E-Safety Policy;

di essere consapevole che, a seguito di violazione volontaria delle regole in esso contenute, la Scuola avrà il diritto di sospendere l'accesso ad Internet e di adottare le sanzioni disciplinari previste.

Pertanto, il/la sottoscritto/a

si impegna a:

utilizzare le Tecnologie dell' Informazione e della Comunicazione (TIC) e la navigazione in internet in modo responsabile, secondo le regole previste dal Documento di E-Safety Policy

Firma .....

Cornaredo .....

Allegato 7

Documento di E-Safety Policy: Assunzione di responsabilità da parte di Docenti e altro Personale della Scuola

Il/La sottoscritto/a ....., dipendente dell' Istituto Comprensivo Da Vinci Cornaredo in qualità di .....

dichiara:
di aver letto e compreso il Documento di E-Safety Policy;

di essere consapevole delle responsabilità connesse all'uso delle Tecnologie dell' Informazione e della Comunicazione (TIC) nella scuola. Pertanto,

il/la sottoscritto/a

si impegna a:

tenere riservate le credenziali di accesso al sistema;
modificare la password periodicamente;
segnalare tempestivamente eventuali perdite di riservatezza;
utilizzare i computer e gli accessi esclusivamente per attività inerenti il proprio servizio e l'aggiornamento professionale; segnalare eventuali anomalie;

vigilare sul corretto utilizzo degli strumenti informatici e della navigazione in rete da parte degli alunni.

Firma

Cornaredo .....

Allegato 8

Patto BYOD (Bring Your Own Device - Porta il tuo dispositivo)

DICHIARAZIONI DEI GENITORI

Il /La sottoscritto/a …….

genitore dell'alunno/a……

frequentante la classe ….. della scuola ……

DICHIARA

di essere al corrente che, in ambito scolastico, i docenti introdurranno, a fianco degli strumenti e dei materiali didattici in uso a scuola, l'utilizzo di applicazioni, contenuti e servizi fruibili in locale e in Internet tramite dispositivi elettronici (device) propri;

di collaborare con i docenti nel responsabilizzare i ragazzi sulle modalità di accesso a internet e sulle regole a cui attenersi.

AUTORIZZA LA SCUOLA

a creare un account personale al proprio figlio/a che permette l'accesso alle condivisioni on line e che include strumenti di comunicazioni (posta elettronica, video-chiamate). Lo strumento permette di ricevere ed inviare messaggi e comunicazioni solo all'interno del dominio della scuola (ovvero con gli altri studenti e con i docenti della scuola);

al trattamento dei dati personali del proprio figlio (comprendendo anche fotografie e videoriprese) nella documentazione online delle attività didattiche svolte. L'accesso a queste pubblicazioni sarà consentito esclusivamente agli utenti del dominio della scuola (alunni, famiglie, docenti, dirigente scolastica, uffici).

Data ……

Firma del/i genitore/i

---------- ----------

Allegato 8bis

PATTO BYOD (Bring Your Own Device - Porta il tuo dispositivo)

GENITORI

Il / La sottoscritto/a ……

genitore dell'alunno/a……

frequentante la classe ….. della scuola …….

AUTORIZZA IL/LA PROPRIO/A FIGLIO/A

a portare a scuola il proprio dispositivo (specificare marca e modello accanto alla tipologia):

TABLET _

SMARTPHONE_ _

VIDEO-GIOCO MULTIMEDIALE_ _

MICROFONO WIRELESS_ _

ALTRO_ _

che sarà usato dallo studente a scuola, in modo individuale o in gruppo, per attività ed esperienze di apprendimento in rete, quali lo scambio e la produzione di materiali condivisi, con la guida e la supervisione dei docenti.

DICHIARA

che durante la permanenza a scuola del dispositivo il proprio figlio sarà responsabile della sua custodia e del suo uso corretto, secondo le regole e le disposizioni concordate con gli insegnanti.

Data ……

firma del/i genitore/i

_____ _____