ISTITUTO COMPRENSIVO 1 VALDAGNO
Via Pasubio 171 – 36078 Valdagno (VI) - Tel. 0445-410428 – Fax 0445-426014
Codice Fiscale: 94006060241 – Codice Ministeriale: VIIC82800V
Indirizzi e-mail: viic82800v@istruzione.it; – P.E.C.: viic82800v@pec.istruzione.it
Sito web: www.icvaldagno1.gov.it

in collaborazione con

PROTOCOLLO DI E-SAFETY

Aggiornamento per l'anno scolastico 2019-2020

1. La necessità di una polizza di sicurezza informatica **2**
Condivisione e comunicazione della Policy all'intera comunità scolastica 3
Gestione delle infrazioni alla Policy 4
Monitoraggio dell'implementazione della Policy e suo aggiornamento 4
Integrazione della Policy con Regolamenti esistenti. 5

2. Formazione e Curricolo 8
Curricolo sulle competenze digitali per gli studenti 8
Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica 8
Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali 9
Sensibilizzazione delle famiglie 9

3. Gestione dell'infrastruttura e della strumentazione ICT della scuola 9
Accesso ad Internet e gestione accessi 9
E-mail 10
Blog e Sito web della scuola 10
Protezione dei dati personali 10

4. Strumentazione personale (gestione degli strumenti personali: cellulari, tablet, …) 10
Per gli studenti 10
Per i docenti e per il personale della scuola 11

5. Prevenzione, rilevazione e gestione dei casi 11
Prevenzione 10
Rilevazione 12
Gestione dei casi 13

6. Allegati (a cura della scuola) 14

1. La necessità di una polizza di sicurezza informatica

Scopo dell'e-Policy

La finalità dell'E-Safety Policy è:

- stabilire i principi fondamentali della comunità scolastica per quanto riguarda l'utilizzo delle tecnologie;
- salvaguardare e proteggere i bambini, i ragazzi e il personale dell'Istituto;
- guidare il personale della scuola affinché lavori in modo sicuro e responsabile con Internet;
- impostare chiare aspettative di comportamento per un uso responsabile di Internet a scopo didattico, personale o ricreativo;
- gestire tramite un protocollo di segnalazione eventuali abusi online, come il cyberbullismo;
- garantire che tutti i membri della comunità scolastica siano consapevoli del fatto che il comportamento illecito o pericoloso è inaccettabile e che per contrastarlo saranno intraprese le opportune azioni disciplinari e giudiziarie.

Le principali aree di rischio per la nostra comunità scolastica riguardano i seguenti ambiti:

- **contenuto:** esposizione a contenuti e siti web non coerenti con le finalità educative di Istituto, problemi legati all'autenticità e all'esattezza dei contenuti online;
- **contatto:** *grooming* (adescamento), cyberbullismo in tutte le sue forme, furto di identità;
- **condotta:** privacy (ad es. divulgazione di informazioni personali), reputazione online, diritti e doveri degli internauti (rudimenti di Cittadinanza Digitale), salute e benessere (quantità di tempo speso online su Internet o giochi), *sexting* (invio e ricezione di immagini personali intime), il rispetto del Copyright.

Ruoli e Responsabilità (di tutti gli attori della Comunità Scolastica)

RUOLO	RESPONSABILITÀ
Il Dirigente Scolastico	– promuovere l'utilizzo sicuro dei dispositivi multimediali e dell'accesso alla rete; – promuovere la formazione del personale su potenzialità e rischi della rete; – dare attuazione al protocollo di e-safety policy e promuoverne l'eventuale aggiornamento; – intrattenere i rapporti con le agenzie competenti e le autorità locali; – promuovere il coordinamento tra le figure istituzionalmente preposte all'utilizzo delle TIC a scuola (Responsabile della Sicurezza, Amministratore di sistema e Animatore Digitale).
Amministratore di sistema (est.)	– operare coerentemente con l'incarico ricevuto in ordine alla realizzazione delle misure minime di sicurezza ICT.
L'Animatore Digitale ed il suo team	– coordinarsi con i responsabili della sicurezza per la formazione sui temi della sicurezza online; – monitorare e rilevare le problematiche relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola; – dotare di password i pc delle aule.
I docenti	– educare gli alunni ad un uso responsabile della rete; – informare gli alunni sulle procedure da seguire per la segnalazione di atti di bullismo e cyberbullismo;

	– informare gli alunni sulle conseguenze degli atti di cyberbullismo; – informarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet; – segnalare al Referente Bullismo di ciascun plesso episodi di presunto bullismo e cyberbullismo; – usare comportamenti sicuri, responsabili e professionali nell'uso della tecnologia; – non allontanarsi dalla postazione senza aver effettuato il logout come "utente docente" dai pc utilizzati; – non salvare sui dispositivi della scuola dati personali; – comunicare ai genitori eventuali problemi o disagi espressi dagli alunni a scuola e connessi all'uso della rete internet.
Il personale scolastico	– usare comportamenti sicuri, responsabili e professionali nell'uso della tecnologia; – contribuire a promuovere politiche di e-safety; – essere consapevoli dei problemi di sicurezza online connessi con l'uso di dispositivi multimediali (es. smartphone, tablet, fotocamere e videocamere digitali, telefoni cellulari, fotocamere e dispositivi portatili); – segnalare qualsiasi sospetto abuso informatico alle figure di sistema.
Gli alunni	– utilizzare correttamente i dispositivi multimediali e internet; – conoscere le linee guida dell'e-safety policy; – capire l'importanza di segnalare ad adulti di riferimento eventuali abusi o l'uso improprio di internet e materiale multimediale; – sapere quali azioni intraprendere se in prima o terza persona dovessero sentirsi preoccupati o vulnerabili utilizzando internet; – conoscere e rispettare il regolamento della scuola sull'uso dei dispositivi multimediali, anche nelle uscite scolastiche; – conoscere l'importanza di adottare buone pratiche di sicurezza on-line quando si usano le tecnologie digitali per non correre rischi; – utilizzare i dispositivi tecnologici personali esclusivamente su autorizzazione del docente e solo per specifiche attività didattiche.
I genitori	– conoscere e sostenere le linee di condotta della scuola nel promuovere la sicurezza online; – condividere l'e-Safety Policy, e accettarla esplicitamente firmando il patto di corresponsabilità educativa; – conoscere le linee di intervento in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di internet.

Condivisione e comunicazione della Policy all'intera comunità scolastica

L'E-Safety Policy d'Istituto si applica a tutti coloro che hanno accesso alla rete scolastica.
In caso di comportamenti e situazioni che mettono a rischio la sicurezza e la privacy dei minori, la scuola ha il compito di attivarsi.
Il documento viene reso pubblico tramite:

- affissione in tutte le aule e laboratori con accesso a Internet delle fondamentali regole per la sicurezza informatica;
- pubblicazione del documento di e-Safety Policy nel sito web della scuola;

Gestione delle infrazioni alla Policy

Disciplina degli alunni
Gli ammonimenti della scuola, pensati in un'ottica inclusiva, sono proporzionati alle circostanze, secondo la seguente gradualità:

- richiamo verbale;
- richiamo scritto con annotazione sul libretto personale e sul registro elettronico;
- convocazione dei genitori da parte degli insegnanti;
- convocazione dei genitori da parte del Dirigente Scolastico.

Contestualmente sono messi in atto interventi di carattere educativo, quali la ridefinizione delle regole sociali della convivenza comune, la promozione di rapporti amicali e della solidarietà, il riconoscimento e la gestione delle emozioni (empatia), attività e lavori socialmente utili.
Ove il fatto costituisca reato si provvede alla segnalazione alle autorità competenti (Polizia, Carabinieri, Procura della Repubblica).

Disciplina del personale scolastico
Il Dirigente Scolastico può controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a internet. Eventuali infrazioni verranno trattate secondo le disposizioni previste dalla legge e dai contratti di lavoro.

Disciplina dei genitori
E' importante che i genitori segnalino alla scuola eventuali episodi di cyberbullismo di cui venissero a conoscenza ed avvenuti in contesto scolastico.
I genitori sono responsabili di materiali inadatti al contesto scolastico introdotti a scuola dai propri figli. I genitori si assumono ogni responsabilità circa la divulgazione, la condivisione e un uso non consentito dalla legge di qualsiasi materiale (fotografie, video, registrazioni e/o materiali personali) relativo agli alunni o da questi detenuto.

Monitoraggio dell'implementazione della Policy e suo aggiornamento

L'E-Safety Policy viene aggiornata qualora l'Istituto ne ravvisi la necessità. Tutte le modifiche, deliberate dal Collegio Docenti, vengono archiviate sulla base del seguente documento:

MODULO PER LA REVISIONE E L'IMPLEMENTAZIONE DELL'E-SAFETY POLICY	
VERSIONE n°……	ANNO SCOLASTICO ……
AUTORE DELLE MODIFICHE:	……
DELIBERA COLLEGIO DOCENTI:	……..
CONTENUTI MODIFICATI	
TESTO PRECEDENTE	TESTO RETTIFICATO
…….. …… …….. ……	…….. …… …… ……

Integrazione della Policy con Regolamenti esistenti.

L' E-Policy integra il *Regolamento d'Istituto* con l'inserimento della seguente norma:
"Utilizzo del laboratorio di Informatica, delle postazioni di lavoro e dell'utilizzo di Internet."

Disposizioni sull'uso del laboratorio d'informatica

1. Le apparecchiature presenti nella scuola sono un patrimonio comune: vanno utilizzate con il massimo rispetto.
2. Il laboratorio può essere utilizzato esclusivamente per attività di insegnamento e di formazione.
3. L'ingresso degli allievi nei laboratori è consentito solo in presenza dell'insegnante.
4. Il docente accompagnatore è responsabile del corretto uso didattico di hardware e software.
5. Nel laboratorio è consentito utilizzare dispositivi personali (cd, dvd, chiavette usb) solo su autorizzazione del docente e previa scansione antivirus del dispositivo.
6. Il laboratorio non deve mai essere lasciato aperto o incustodito quando nessuno lo utilizza.
7. All'uscita dal laboratorio, è compito di chi ne ha usufruito lasciare l'aula in ordine e spegnere correttamente i dispositivi informatici utilizzati.
8. In caso di malfunzionamento o guasto dei computer l'insegnante deve darne tempestiva segnalazione al Responsabile del Laboratorio.
9. L'accesso al laboratorio è regolato da un registro cartaceo.
10. Per motivi di manutenzione straordinaria, in caso di guasti o di virus, i PC possono essere formattati senza preavviso.
11. Il Responsabile di laboratorio che verifichi un uso delle TIC contrario a disposizioni di legge o del regolamento interno deve darne comunicazione per iscritto al Dirigente Scolastico.

Disposizioni sull'uso dei software nelle postazioni pc d'Istituto

1. I software installati sono ad esclusivo uso didattico.
2. In base alle leggi che regolano la distribuzione delle licenze, i software presenti in laboratorio non sono disponibili per il prestito individuale.
3. Solo l'amministratore di sistema è autorizzato all'installazione di nuovi software.

Accesso a Internet

1. **L'accesso a Internet è consentito alle classi esclusivamente sotto la supervisione del docente.**
2. L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet. In caso di responsabilità da parte di un minore, ne risponde la famiglia.

Il nostro Istituto vieta l'uso di qualsiasi dispositivo digitale personale durante l'orario scolastico, tranne nel caso in cui venga proposta un'attività didattica da parte dell'insegnante, in sua presenza e sotto la sua supervisione. Diversamente, è fatto divieto assoluto agli alunni di utilizzare il proprio smartphone in classe, nei corridoi, nei bagni e in qualsiasi altro locale della scuola, compreso il cortile, durante la ricreazione. Il cellulare dovrà essere tenuto spento e riposto dentro lo zaino dal momento dell'ingresso fino alla fine delle lezioni.

Stiamo anche valutando la predisposizione in tutte le aule di cassette di sicurezza dove raccogliere tutti i telefoni, spenti, i quali verranno riconsegnati agli alunni al momento di lasciare l'istituto al termine delle lezioni.
La violazione di tale divieto configura un'infrazione disciplinare rispetto alla quale la scuola è tenuta ad applicare apposite sanzioni, in applicazione della normativa vigente (DPR. n. 249/1998, DPR. n. 235/2007, Direttiva Ministeriale 15.03.2007).
Si ricorda che i genitori rispondono direttamente dell'operato dei propri figli nel caso in cui gli stessi violino i doveri sanciti dal Regolamento di Istituto.

Le sanzioni, sono individuate dal nostro istituto secondo il criterio della gradualità, in modo tale da garantire, con rigore ed in maniera efficace il rispetto delle regole, della cultura della legalità e della convivenza civile.
Docenti, personale amministrativo ed ausiliario hanno doveri deontologici e professionali sia di vigilanza sui comportamenti degli studenti in tutti gli spazi scolastici che di tempestiva segnalazione alle autorità competenti di eventuali infrazioni.

Mancanza disciplinare	Frequenza	Sanzione disciplinare	Organo competente
L'alunno tiene lo smartphone spento in vista sul banco.	1^ volta	Richiamo verbale (con annotazione sul registro elettronico per informare il Consiglio di classe e comunicazione alla famiglia sul libretto).	Docente
	2^ volta	Annotazione sul registro elettronico con comunicazione alla famiglia sul libretto personale. Comunicazione al DS. Convocazione della famiglia.	Docente Coordinatore Dirigente Scolastico
L'alunno non ha lo smartphone spento.	1^ volta	Annotazione sul registro elettronico con comunicazione alla famiglia sul libretto personale.	Docente
	2^ volta	Annotazione sul registro elettronico con comunicazione alla famiglia sul libretto personale. Requisizione dello smartphone e sua riconsegna alla fine delle lezioni direttamente al genitore, che viene tempestivamente informato del fatto dalla segreteria/docente. Nel caso questo non fosse possibile,il dispositivo viene restituito all'alunno. Comunicazione al DS.	Docente Coordinatore Dirigente Scolastico
	3^ volta	Annotazione sul registro elettronico. Comunicazione al DS. Sequestro dello smartphone e sua riconsegna direttamente al genitore. Convocazione della famiglia. In seguito provvedimento disciplinare di sospensione dalle lezioni da un giorno a un massimo di 5 giorni, a discrezione del Consiglio di Classe.	Docente Coordinatore Dirigente Scolastico Consiglio di Classe
L'alunno si rifiuta di riporre lo smartphone spento nello zaino o di consegnarlo all'insegnante.		Annotazione sul registro elettronico con comunicazione alla famiglia sul libretto personale. Comunicazione al DS. Convocazione della famiglia.	Docente Docente Coordinatore Dirigente Scolastico
L'alunno utilizza il cellulare a scuola per chiamate e/o messaggistica o altri usi non consentiti (giochi, ascolto musica, uso casse, chat, ecc.)		Annotazione sul registro elettronico con comunicazione alla famiglia sul libretto personale. Comunicazione al DS. Convocazione della famiglia. Provvedimento disciplinare di allontanamento durante la ricreazione, da trascorrersi davanti alla Presidenza, per un numero di giorni da definire, con gradualità.. In alternativa, o in caso di recidive, provvedimento disciplinare di sospensione dalle lezioni da un giorno a un massimo di 5 giorni, a discrezione del Consiglio di Classe	Docente Coordinatore Dirigente Scolastico Consiglio di Classe
L'alunno usa dei dispositivi elettronici non autorizzati durante una		Ritiro della verifica e valutazione gravemente insufficiente della stessa. Nota sul registro elettronico, con comunicazione alla famiglia sul libretto.	Docente

prova.			
L'alunno effettua a scuola riprese audio/video/foto non autorizzate.		Annotazione sul registro elettronico con comunicazione alla famiglia sul libretto personale. Comunicazione al DS. Convocazione della famiglia. In seguito provvedimento disciplinare di sospensione dalle lezioni da 3 giorni a un massimo di 15 giorni, a discrezione del Consiglio di Classe. Possibilità di denuncia per violazione della privacy.	Docente Coordinatore Dirigente Scolastico Consiglio di Classe
L'alunno diffonde anche in rete e nei social network immagini/video/audio non autorizzati effettuati a scuola	1^ volta	Annotazione sul registro elettronico con comunicazione alla famiglia sul libretto personale. Comunicazione al DS. Convocazione della famiglia. In seguito provvedimento disciplinare di sospensione dalle lezioni fino a 15 giorni, secondo un principio di gradualità. Possibilità di denuncia per violazione della privacy.	Docente Coordinatore Dirigente Scolastico Consiglio di Classe

Nei casi di estrema gravità, in cui vi siano fatti di rilevanza penale o situazioni di rischio per l'incolumità delle persone, anche riconducibili a episodi di violenza fisica o psichica o a gravi forme di bullismo, la sanzione prevede la sospensione fino a quindici giorni e la segnalazione al più opportuno organo di garanzia.

Le sospensioni, eccetto nei casi più gravi di violazione della privacy, possono essere sempre commutate - a discrezione del Consiglio di Classe - in attività a favore della comunità o comunque orientata al perseguimento di un interesse generale della comunità scolastica (quali la pulizia delle aule, piccole manutenzioni, svolgimento di attività di assistenza o di volontariato nell'ambito della comunità scolastica, ...).

2. Formazione e Curricolo

Il Piano Nazionale Scuola Digitale (PNSD) normato dalla Legge 107 del 2015, ha l'obiettivo di modificare gli ambienti di apprendimento per rendere l'offerta formativa di ogni istituto coerente con i cambiamenti della società e con le esigenze e gli stili cognitivi delle nuove generazioni. Il PNSD, con valenza pluriennale, vuole essere un'opportunità per innovare la Scuola, adeguandone non solo le dotazioni tecnologiche, ma anche le metodologie e le strategie didattiche.
Il D.M. 851 del 27 ottobre 2015, in attuazione dell'art.1, comma 56 della legge 107/2015, invita infatti a:

- migliorare le competenze digitali degli studenti anche attraverso un uso consapevole delle stesse;
- implementare le dotazioni tecnologiche per migliorare gli strumenti didattici e laboratoriali;
- favorire la formazione dei docenti ai fini dell'innovazione didattica;
- individuare un Animatore Digitale ed un team per l'innovazione che supporti ed accompagni adeguatamente l'attività didattica;
- partecipare a bandi nazionali ed europei per finanziare le suddette iniziative.

Curricolo sulle competenze digitali per gli studenti

Il Curricolo sulle competenze digitali della scuola del Primo Ciclo di Istruzione è trasversale alle discipline previste dalle Indicazioni Nazionali: la competenza digitale è ritenuta dall'Unione Europea competenza chiave, per la sua importanza e pervasività nel mondo d'oggi.
Avere competenza digitale significa padroneggiare le nuove tecnologie, ma soprattutto usarle con "autonomia e responsabilità" nel rispetto degli altri.

Nell'ambito del PNSD l'Istituto 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, tra cui:

- progettare attività e laboratori di Coding;
- sviluppare strategie per insegnare a valutare e verificare le informazioni per accettarne l'esattezza;
- capire la necessità di mettere in atto un comportamento corretto anche quando si utilizza un ambiente online;
- sapere che le identità online possono essere false e ingannevoli;
- comprendere che le informazioni personali pubblicate online sono vulnerabili;
- conoscere le principali regole che tutelano la privacy delle persone;
- con particolare attenzione al web, conoscere le principali regole del copyright;
- comprendere l'impatto di bullismo online, sexting, grooming e sapere come cercare aiuto in caso di pericolo;
- sapere come segnalare eventuali abusi on-line e come chiedere aiuto agli adulti.

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

Tra i principali vantaggi legati all'utilizzo delle TIC nella didattica vi sono l'incremento della motivazione e del coinvolgimento attivo da parte degli alunni, la facilitazione dei lavori di gruppo e del confronto fra pari, l'arricchimento della proposta didattica e supporto all'apprendimento per gli studenti con Bisogni Educativi Speciali.

Il nostro Istituto intende implementare e incoraggiare la formazione personale dei docenti con corsi sull'uso delle TIC in ambito territoriale (ad esempio con iniziative promosse dall'Amministrazione e dalle scuole polo), ma anche interni alla scuola stessa, avvalendosi delle risorse di docenti esperti. Supporta anche l'auto aggiornamento dei singoli docenti.

Eventuale 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.

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

La formazione dei docenti sull'utilizzo consapevole e sicuro di internet può prevedere momenti di autoaggiornamento e di formazione personale o collettiva.

Nell'ambito del PNSD l'IC Valdagno 1 prevede:

- l'individuazione di un Animatore Digitale che affiancherà il Dirigente Scolastico nell'attuazione degli obiettivi e delle innovazioni previste dal PNSD;
- la formazione dei docenti all'utilizzo del registro e dello scrutinio elettronici;
- la somministrazione di un questionario rivolto ai docenti per la rilevazione dei bisogni "digitali";
- la realizzazione/ampliamento della rete WI-FI/LAN nei plessi dell'Istituto;
- la ricognizione e la messa a punto delle dotazioni digitali;
- iniziative di formazione, in particolare rivolte allo sviluppo e alla diffusione del Coding e del pensiero computazionale;
- l'utilizzo consapevole da parte del personale docente e di segreteria dei dati sensibili o personali e la prassi di crittografare i dati dove la sensibilità richiede protezione degli stessi;
- la formazione dei docenti in materia di sicurezza on-line attraverso corsi di aggiornamento;
- l'informazione a tutto il nuovo personale che lavori nell'istituto sui contenuti dell'e-Policy.

Sensibilizzazione delle famiglie

La scuola si impegna:

- alla diffusione delle informazioni e delle procedure contenute nel documento di e-safety policy;

- ad offrire incontri e conferenze con esperti;
- a fornire sul sito www.icvaldagno1.gov.it un link per informazioni utili contro il cyberbullismo come sostegno per alunni e famiglie.

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

Accesso ad Internet e gestione accessi

La scuola può controllare periodicamente i file utilizzati, i file temporanei e i siti visitati da ogni macchina (cronologia).
E' vietato installare e scaricare da Internet software non autorizzati dall'amministrazione.
Al termine di ogni collegamento la connessione deve essere chiusa.
Controlli tramite antivirus sono condotti periodicamente sui computer e sulle unità di memorizzazione di rete.
L'utilizzo di unità di archiviazione e chiavette usb è autorizzata, previa opportuna scansione antivirus, per evitare qualsiasi tipo di infezione alla rete d'Istituto.
La scuola dispone in tutte le sue sedi di una rete internet, cui accedono i computer delle aule e dei laboratori (rete didattica) separatamente da quelli dell'amministrazione (rete segreteria);
La rete interna della sede centrale e i plessi della primaria sono protetti da Firewall. Le postazioni sono protette con sistemi antivirus regolarmente aggiornati. Su questi dispositivi non è garantito alcun servizio di backup. Per quanto concerne la rete amministrativa, lo storage è garantito da backup automatico su altra postazione. L'Istituto dispone anche di una rete con tecnologia senza fili. L'ottenimento delle credenziali è riservato ai docenti e al personale dell'Istituto. Le regole di comportamento sono analoghe a quelle per la connessione alle reti cablate di Istituto.
I computer presenti nelle singole aule e nel laboratorio di informatica sono regolati da password per l'accesso alla Rete. Non è previsto l'accesso al wi-fi della scuola per gli studenti, che possono utilizzare la rete esclusivamente in presenza dei docenti, attraverso gli strumenti informatici in dotazione nella scuola.

E-mail

L'account di posta elettronica della scuola è quello istituzionale, utilizzato dagli uffici amministrativi. Poiché *spam* (email e messaggistica istantanea online indesiderata), *phishing* (frode online per sottrarre con inganno numeri di carte di credito, password e informazioni personali) e virus allegati possono rendere le mail pericolose, si utilizzeranno precauzioni informatiche, tra cui adeguati Antivirus, per proteggere utenti e sistemi nella scuola.

Blog e Sito web della scuola

L'Istituto dispone di un proprio spazio web con il sito **www.icvaldagno1.gov.it.**
Il Registro Digitale Nuvola, già in uso, prevede una sezione dedicata alle famiglie che prossimamente sarà attivata per la scuola Secondaria di primo grado.
La gestione del sito della scuola, la realizzazione, la progettazione e la rispondenza alle normative sono attualmente a cura della segreteria e di Nuvola-Madisoft.
La scuola detiene i diritti d'autore (tramite protocollo informatico) dei documenti che si trovano sul proprio sito. Le informazioni ivi pubblicate, relative alle persone, rispettano le norme vigenti sulla privacy. La scuola pubblica sul proprio sito web i contenuti valutati come pertinenti alle finalità educative istituzionali.

Protezione dei dati personali

Il personale scolastico è "incaricato del trattamento" dei dati personali nei limiti delle operazioni dello svolgimento della propria funzione.

I genitori sono avvisati tramite informativa o specifica richiesta di autorizzazione per l'utilizzo degli stessi, ad eccezione dei trattamenti istituzionali obbligatori.

4. Strumentazione personale (gestione degli strumenti digitali personali)

Per gli studenti

La scuola non consente l'utilizzo del cellulare personale degli alunni all'interno dell'istituto e in orario scolastico; per assolvere ad ogni comunicazione urgente è disponibile il telefono della scuola supervisionato dal personale scolastico addetto.
E' consentito l'uso dello smartphone solo previa autorizzazione del docente.

Per i docenti e per il personale della scuola

Durante le ore di lezione è consentito l'uso dello smartphone e di altri dispositivi elettronici personali solo a scopo didattico ed integrativo di quelli scolastici disponibili.

5. Prevenzione (1), rilevazione (2) e gestione dei casi (3)

1. Prevenzione

Rischi potenziali

Considerate le molteplici problematiche sociali che si manifestano in rete e che interessano o coinvolgono direttamente e indirettamente la scuola (bullismo, cyberbullismo, grooming, sexting, pedopornografia, le violazioni della Privacy, il furto di identità, il gioco d'azzardo online, le pressioni psicologiche di varia natura, sextortion, abusi e violenze,…), è fondamentale agire sulla prevenzione dei comportamenti a rischio e sulla formazione/informazione nei confronti dell'intera comunità scolastica.
E' importante che la scuola sia messa quanto prima al corrente di eventuali criticità, e che attraverso colloqui, apposite schede di osservazione o relazioni *ad hoc*, mantenendo un contatto diretto con le famiglie, l'ULSS e le autorità competenti (Polizia Postale, Carabinieri, Garante della Privacy dell'Infanzia, la Procura), possa contribuire ad agire tempestivamente per risolvere i problemi.
Purtroppo, quando l'azione preventiva risulta tardiva o non efficace, occorre passare direttamente al contrasto dei fenomeni sopracitati.

Azioni

Per individuare eventuali problemi è fondamentale tenere controllata la situazione emotiva dei minori potenzialmente coinvolti, registrando eventuali improvvisi cambi d'umore, variazioni del rendimento scolastico e di abitudini di vita, informandosi anche - se possibile - circa le modalità e l'intensità dell'uso dei dispositivi informatici e della rete internet, nell'ottica di intraprendere eventuali azioni necessarie a tutelarne la sicurezza e l'incolumità.
Per garantire una corretta gestione delle criticità è importante che tutto il personale scolastico, le famiglie e gli alunni sappiano che è possibile chiedere aiuto o informazioni attraverso il telefono, la chat, l'email. Materiali e informazioni utili sono disponibili anche navigando su piattaforme dedicate, come quella di *Generazioni Connesse*.
Per chiunque sia coinvolto in una situazione di violenza, bullismo o cyberbullismo, oltre agli adulti di riferimento, esistono differenti modalità e strumenti per chiedere informazioni, supporto e aiuto, tra cui:

- due servizi messi a disposizione dal Safer Internet Center italiano: sono il "*Clicca e Segnala*" di Telefono Azzurro e "*STOP-IT*" di Save the Children. Una volta ricevuta la segnalazione, gli operatori procederanno a coinvolgere le autorità competenti in materia.

- **1.96.96:** numero per l'helpline e la chat del Telefono Azzurro: essa accoglie qualsiasi richiesta di ascolto e di aiuto da parte di bambini/e e ragazzi/e fino ai 18 anni o di adulti che intendono

confrontarsi su situazioni di disagio/pericolo in cui si trova un minorenne. Il servizio è riservato, gratuito e sicuro, dedicato ai giovani o ai loro familiari che possono chattare, inviare e-mail o parlare al telefono con professionisti qualificati relativamente a dubbi, domande o problemi legati all'uso delle nuove tecnologie digitali e alla sicurezza online. Fornisce il supporto per la hotline (ovvero la denuncia e il contrasto del fenomeno) e l'helpline (per la gestione e la presa in carico dello stesso).

- **114:** Emergenza Infanzia: è un modello multiagency che, oltre all'utente coinvolto, può attivare anche le Forze dell'Ordine, i Servizi Sociali, le agenzie del territorio, le procure e i tribunali, il MIUR.

- **116.000:** Numero Unico Europeo per minori scomparsi, o minori stranieri non accompagnati.

Il contrasto del fenomeno è una priorità della nostra scuola e delle istituzioni; a seguito della presa in carico di situazioni, verificatesi a scuola, potenzialmente pericolose o in fase iniziale può essere necessario (previa comunicazione alla famiglia) provvedere alla segnalazione del caso o alla denuncia dell'illecito alle autorità competenti, tramite gli appositi protocolli allegati a questo documento.
E' doveroso contattare la Polizia se si ritiene che il materiale offensivo sia illegale.
In caso di foto e video pornografici di cui la scuola dovesse venire a conoscenza, ritirare il telefonino o altri dispositivi ed evitare di eseguire download o riprodurne copie poiché ciò è reato per chiunque.
Nei casi di una condotta incauta in Internet (ad esempio la diffusione di dati personali, di materiali sensibili o lesivi dei diritti fondamentali di ciascuno) è indispensabile che il minore e la sua famiglia si attivino per rimuovere i contenuti inappropriati quanto prima (contattando il service provider del sito e/o tramite denuncia alla Polizia Postale).
A tal proposito si rimanda al riferimento legislativo vigente, Art. 2, "*Tutela della dignità del minore*", comma 1 e seguenti, della Legge 29 maggio 2017, n. 71 il quale prevede che

> "C*iascun minore ultraquattordicenne, nonché ciascun genitore o soggetto esercente la responsabilità del minore che abbia subito taluno degli atti di cui all'articolo 1, comma 2, della presente legge, può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco di qualsiasi altro dato personale del minore, diffuso nella rete internet, previa conservazione dei dati originali, anche qualora le condotte di cui all'articolo 1, comma 2, della presente legge, da identificare espressamente tramite relativo URL, non integrino le fattispecie previste dall'articolo 167 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n.196, ovvero da altre norme incriminatrici."*

Per episodi o atti che non avvengono in orario e in sede scolastica, la famiglia deve rivolgersi direttamente alle autorità competenti. Ciò non toglie che la scuola, per quanto di sua competenza, possa contribuire ad accogliere la sofferenza e il disagio delle parti coinvolte, attraverso lo sportello di spazio ascolto, gestito dalla psicologa della scuola, o mediante attività specifiche (iniziative per l'inclusione, l'empatia, il supporto tra pari, ecc...) valutate caso per caso.

2. Rilevazione

Che cosa segnalare in materia di cyberbullismo

La recente normativa delinea chiaramente ciò che è perseguibile a norma di legge quando si parla di cyberbullismo. L'art.1. comma 2 della Legge 29 maggio 2017, n. 71 "*Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo*", recita:

> "*ai fini della presente legge, per «cyberbullismo» si intende qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in*

danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti online aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo".

Nel caso a scuola gli insegnanti notassero o fossero informati di alcuni comportamenti non responsabili o potenzialmente pericolosi posti in essere da uno o più studenti, può rendersi necessaria una convocazione dei genitori o una relazione scritta al Dirigente Scolastico il quale valuterà le possibili azioni conseguenti.
Inoltre il nostro istituto offre sul sito e in allegato a questo documento una **scheda per la segnalazione della violazione a Garante per la Privacy (allegato D)**.

Riconoscere e intervenire in situazioni di bullismo e cyberbullismo non è semplice.

Disporre di adeguati strumenti condivisi da tutta la scuola è fondamentale per affrontare in modo sistematico le criticità.

Come segnalare
E' importante che a scuola, in tutti i plessi, siano facilmente reperibili la **scheda di osservazione (allegato B)** per fenomeni afferenti a bullismo e cyberbullismo e la **scheda per la segnalazione del presunto caso (allegato C)** di bullismo e cyberbullismo.
La compilazione degli stessi, da parte della persona coinvolta o per mano di terzi, è il primo passaggio per una corretta gestione di un eventuale problema. E' altresì possibile comunicare direttamente con gli insegnanti della Commissione Bullismo, con la psicologa dello sportello di spazio-ascolto, la vicepreside o il Dirigente Scolastico, che si faranno da tramite.
Conservare le prove, è utile per fornire elementi utili a cercare di comprendere l'accaduto. Eventuali testimonianze dirette o indirette, devono comunque essere comunicate alla Commissione Bullismo, che deciderà come procedere.
Quando si viene a conoscenza di un problema di bullismo e cyberbullismo non è opportuno che il singolo intraprenda iniziative personali, come ad esempio interrogare bulli e/o le vittime: occorre rivolgersi alla Commissione che, progettando l'intervento e confrontandosi anche con i docenti di classe, prenderà in carico il problema.
La segnalazione alle autorità competenti può avvenire su iniziativa della famiglia del minore coinvolto o può essere fatta dalla scuola.

3. Gestione dei casi: il *Protocollo d'azione*

La nostra scuola ha approvato un ***protocollo d'azione*** **(allegato A)** in quattro fasi per la segnalazione e la presa in carico di situazioni problematiche:

1- RICEZIONE DELLA SEGNALAZIONE. La ricezione e l'accoglienza da parte della scuola di una segnalazione di atti di bullismo e cyberbullismo coincide con la presa in carico di essa da parte del nostro Istituto. Ascolto e garanzia di riservatezza, ove possibile, sono d'obbligo. Generalmente in questa fase è già possibile individuare se si tratta di bullismo/cyberbullismo. La scuola è presente e vicina a chiunque chieda un suo intervento, poiché il benessere della comunità scolastica è una dimensione fondamentale.

2. VALUTAZIONE DELLA SEGNALAZIONE. La segnalazione viene presa in carico dalla Commissione Bullismo. In questa fase possono essere effettuati accertamenti e/o intrapresi, da uno psicologo interno alla scuola o da docente esperto, dei colloqui individuali con le persone coinvolte, nel rispetto della loro privacy e nell'ottica di un'alleanza terapeutica.
La Commissione si riserva di informare la famiglia nel caso di una situazione di effettivo pericolo.

In questa fase si classificheranno le segnalazioni in base alla loro specifica natura, ovvero secondo la tipologia "*dell'immaturità*", "*della prepotenza e della prevaricazione (bullismo)*", "*delle molestie/offese attuate attraverso strumenti tecnologici (cyberbullismo)*" o "*degli abusi*".

3. SCELTA DI INTERVENTO E GESTIONE DEL CASO. La Commissione, in accordo con i coordinatori di classe può valutare se è opportuno gestire il caso individualmente, nel gruppo classe o in piccolo gruppi, alla presenza o meno degli alunni coinvolti, a seconda della linea che si decide di seguire.
Qualora la scuola rilevi una situazione psico-socio-educativa particolarmente problematica, si riserva di convocare i genitori per valutare con loro a quali risorse territoriali rivolgersi.
La scuola, se ne ravvede la necessità, può consigliare le persone coinvolte di rivolgersi allo sportello di spazio-ascolto psicologico dell'Istituto o può supportare la richiesta delle famiglie presso i Servizi Sociali dell'ULSS per la fruizione di servizi socio-educativi comunali e all'ASL di competenza per altri interventi di natura psicologica e psicoterapeutica (Pediatria, Neuropsichiatria, Consultorio Familiare).

4. MONITORAGGIO. E' opportuno che, a *distanza di due settimane e di due mesi* dalle azioni intraprese dalla scuola, venga pensata un'attività di monitoraggio della situazione e del problema segnalato.

6. Allegati (a cura della scuola)

A. Schema riepilogativo del *Protocollo di intervento*;
B. *Scheda di osservazione* di caso;
C. Modulo di segnalazione di presunto bullismo/cyberbullismo (uso interno scuola);
D. *Modulo di segnalazione al Garante per la protezione dei dati personali* in materia di cyberbullismo (per la famiglia).
E. P.U.A. Politica di Uso Accettabile.

Documento a cura della *Commissione Bullismo* dell'IC Valdagno 1.

Valdagno, 06/11/2019

Referente Commissione Bullismo
Magaraggia Chiara Patrizia

_____

Il Dirigente Scolastico Prof.ssa
Dott.ssa Maria Catena Lupo

_____

ISTITUTO COMPRENSIVO 1 VALDAGNO
Via Pasubio 171 – 36078 Valdagno (VI) - Tel. 0445-410428 – Fax 0445-426014
Codice Fiscale: 94006060241 – Codice Ministeriale: VIIC82800V
Indirizzi e-mail: viic82800v@istruzione.it; – P.E.C.: viic82800v@pec.istruzione.it
Sito web: www.icvaldagno1.gov.it

ALLEGATO A

SCHEMA RIEPILOGATIVO DEL **PROTOCOLLO DI INTERVENTO**
PER L'IC VALDAGNO 1

PREVENZIONE E FORMAZIONE

- Attività curricolare di prevenzione, sensibilizzazione e informazione in classe, sui temi del rispetto, dell'empatia, dell'inclusione, del bullismo.

- Interventi di esperti esterni e/o interni.

SOSPETTA SITUAZIONE DI RISCHIO

Presa in carico del problema da parte del docente di classe:

- osservare/ monitorare la situazione con scheda di osservazione
- avviare con prudenza alcuni accertamenti
- compilazione modulo di segnalazione di presunto bullismo/cyberbull
- monitoraggio del caso

EVIDENTE SITUAZIONE DI RISCHIO

Presa in carico del problema da parte della Commissione Bullismo:

- compilazione modulo di segnalazione di presunto bullismo/cyberbull.
- valutazione della segnalazione da parte della Commissione

e in caso di

A) FALSO ALLARME/ SITUAZIONE DI NON BULLISMO:
ascolto nei confronti di chi ha effettuato la segnalazione, monitoraggio della situazione del singolo/della classe, attività mirate di sensibilizzazione e monitoraggio, eventuali colloqui di accertamento (concordati)

B) SITUAZIONE CRITICA/ EMERGENZA:
- accertamenti secondo le modalità concordate con la Commissione
- informare la famiglia e - se necessario - le autorità
- eventuali colloqui con psicologo della scuola o docenti esperti
- individuazione della linea di intervento e sua attuazione
- monitoraggio della situazione

ISTITUTO COMPRENSIVO 1 VALDAGNO
Via Pasubio 171 – 36078 Valdagno (VI) - Tel. 0445-410428 – Fax 0445-426014
Codice Fiscale: 94006060241 – Codice Ministeriale: VIIC82800V
Indirizzi e-mail: viic82800v@istruzione.it; – P.E.C.: viic82800v@pec.istruzione.it
Sito web: www.icvaldagno1.gov.it

ALLEGATO B

SCHEDA DI OSSERVAZIONE PER LA RILEVAZIONE DI EVENTUALI SITUAZIONI PROBLEMATICHE IN CLASSE RICONDUCIBILI A BULLISMO /CYBERBULLISMO

PER L'ALUNNO:.....

1° segnalazione. Il problema è stato osservato da ……..…
Data……. Luogo …….. Orario……..
Nome di chi ha subito: ……. Nome di chi ha agito:..... Descrizione del comportamento/della situazione: ……. ……. ……. (Eventuale) reazione della classe: …… …….
Azione dell'adulto: ○ nessuna ○ richiamo ○ intervento in classe ○ nota sul libretto ○ nota sul registro ○ telefonata/ convocazione della famiglia Attualmente il rendimento scolastico dell'alunno vittima risulta ○ stabile ○ in calo Il suo livello di attenzione/partecipazione in classe è ○ invariato ○ alterato ○ molto alterato
Firma: …….

ISTITUTO COMPRENSIVO 1 VALDAGNO
Via Pasubio 171 – 36078 Valdagno (VI) - Tel. 0445-410428 – Fax 0445-426014
Codice Fiscale: 94006060241 – Codice Ministeriale: VIIC82800V
Indirizzi e-mail: viic82800v@istruzione.it; – P.E.C.: viic82800v@pec.istruzione.it
Sito web: www.icvaldagno1.gov.it

ALLEGATO C

Al Dirigente Scolastico
Alla Commissione Bullismo

PRIMA SEGNALAZIONE DI (PRESUNTO) BULLISMO, CYBERBULLISMO E VITTIMIZZAZIONE

Nome di chi compila la segnalazione: ……	
Data: ……..	
Plesso di Istituto: …….	
1. La persona che segnala il caso di presunto bullismo - cyberbullismo è	
La vittima	……..……..……..……...
Un compagno della vittima (nome)	……..……..……..……..
Madre, padre, tutore della vittima (nome)	……..……..……..……..……...
Insegnante (nome)	…….
Altro (specificare) ……	(nome) ……...
comunica chi sono	
2. la vittima …….	classe :……..
Altre vittime: ……...	classe :……..
Altre vittime: ……...	classe :……..
3. bullo o i bulli (o presunti)	
Nome: ……..	classe :……..
Nome: ……..	classe :……..
Nome: ……..	classe :……..
4. Descrizione breve del problema presentato. Dare esempi concreti degli episodi di prepotenza. ……..….. …….. …….. …….. …… …… ……	
5. <u>Quante volte</u> sono successi gli episodi? ……...…… …… ……...	

ALLEGATO D

Modello per la segnalazione al garante della privacy in materia di cyberbullismo

Al Garante per la protezione dei dati personali
Inviare all'indirizzo e-mail: cyberbullismo@gpdp.it

OGGETTO: segnalazione ai sensi dell'art.2, comma 2, legge 29 maggio 2017, n.71, disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo.

Il/La sottoscritto/a _____([1]), nato/a a _____,
il _____, residente a _____, via/p.za _____,

tel. _____, e-mail/PEC _____ *[inserire recapiti ai quale si può essere contattati e selezionare, di seguito, l'opzione pertinente]*,

- □ minore ultraquattordicenne,
  ovvero
- □ in qualità di esercente la responsabilità genitoriale sul minore _____,
  nato a _____ il _____.

SEGNALA

1. di essere stato/a vittima ovvero che il minore sul quale esercita la responsabilità genitoriale è stato vittima di cyberbullismo [*eliminare la locuzione che non interessa*]. In particolare, i comportamenti posti in essere, **realizzati per via telematica** e di seguito sinteticamente descritti, consistono in [*selezionare la/e fattispecie rilevanti*]
   - □ pressione
   - □ aggressione
   - □ molestia
   - □ ricatto
   - □ ingiuria
   - □ denigrazione
   - □ diffamazione
   - □ furto d'identità
   - □ alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati

ovvero

- □ diffusione di contenuti *on line* aventi ad oggetto il minore ovvero uno o più componenti della famiglia del minore *[rimuovere l'informazione non rilevante]* allo scopo intenzionale e predominante di isolare il minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo.

Riferisce sinteticamente i seguenti fatti:

_____

_____

1Avvertenza: la segnalazione o il reclamo può essere presentata direttamente anche da minori d'età ultraquattordicenni ovvero da chi esercita la responsabilità genitoriale. Pertanto si prega il segnalante/reclamante di fornire le pertinenti informazioni.

_____

_____

_____

che la diffusione di contenuti lesivi dell'interessato/a è avvenuta [*selezionare la casella pertinente*]:

- □ sul sito internet _____ all'indirizzo web [*necessario indicare URL*] _____
- □ *social media* [*necessario inserire individuazione univoca*] _____
- □ altro [*necessario specificare*] _____

Allega i seguenti documenti (ad es. immagini, video, *screenshot*, etc.):

_____

_____

_____

Tanto premesso, [*selezionare l'opzione pertinente*]

- □ considerato che il gestore del sito internet o del *social media* al quale è stata presentata l'istanza allegata per l'oscuramento, la rimozione o il blocco dei dati personali diffusi in internet non ha comunicato entro 24 ore di avere assunto l'incarico di provvedere all'oscuramento, alla rimozione o al blocco richiesto, né vi ha provveduto entro quarantotto ore *[allegare la pertinente documentazione]*;

- □ considerato che non è stato in grado di presentare un'istanza per l'oscuramento, la rimozione o il blocco dei dati personali diffusi in internet al gestore del sito internet o del *social media* non essendo possibile identificare il titolare del trattamento o il gestore del sito internet o del *social media*,

RICHIEDE

di disporre, ai sensi degli articoli 2, comma 2, l. n. 71/2017 nonché 143 e 144, d.lgs. n. 196/2003, il blocco/divieto della diffusione dei dati personali sopra descritti.

Il/La sottoscritto/a dichiara inoltre di *[selezionare la casella pertinente]:*

- □ aver presentato denuncia/querela per i fatti sopra descritti presso _____;
- □ non aver presentato denuncia/querela per i fatti sopra descritti.

ACCONSENTE

Ai sensi e per gli effetti degli articoli 13 e 23 del D.Lgs. 196/03, con la sottoscrizione del presente modulo, al trattamento dei dati personali qui forniti.

Luogo, data | Nome e Cognome

_____ | _____

ISTITUTO COMPRENSIVO 1 VALDAGNO
Via Pasubio 171 – 36078 Valdagno (VI) - Tel. 0445-410428 – Fax 0445-426014
Codice Fiscale: 94006060241 – Codice Ministeriale: VIIC82800V
Indirizzi e-mail: viic82800v@istruzione.it; – P.E.C.: viic82800v@pec.istruzione.it
Sito web: www.icvaldagno1.gov.it

ALLEGATO E

PUA

Politica di Uso Accettabile

-

Integrazione al *Regolamento di Istituto* in merito alla Sicurezza Informatica *ed Uso Consapevole delle TIC nella scuola.*

Introduzione e processo di revisione
L'Istituto Comprensivo Valdagno 1 si è dotato di una politica d'uso accettabile e responsabile di Internet per essere pronto a cogliere i cambiamenti sociali, economici, culturali e tecnologici del contesto in cui opera, in particolare per quanto riguarda la formazione dei cittadini del futuro, destinati a vivere in un ambiente in cui tutto viene gestito attraverso l'utilizzo delle Tecnologie dell'Informazione e della Comunicazione (TIC). Tali tecnologie diventano abilitanti, quotidiane, ordinarie, al servizio dell'attività scolastica e di tutti i suoi ambienti. Il curricolo scolastico prevede che gli studenti imparino a trovare materiale, recuperare documenti e scambiare informazioni utilizzando le TIC.
L'Istituto inoltre intende utilizzare internet per promuovere l'eccellenza in ambito didattico attraverso la condivisione delle risorse, l'innovazione e la comunicazione.
Poiché esiste la possibilità che gli studenti trovino materiale inadeguato e illegale su Internet, l'Istituto prende le precauzioni necessarie per evitare tali inconvenienti. Gli insegnanti hanno il compito di guidare gli studenti verso un uso di Internet accettabile e responsabile.
L'obiettivo principale resta quello di arricchire ed ampliare le attività didattiche, secondo quanto prevede il curricolo scolastico, l'età e la maturità degli studenti.
La PUA verrà revisionata e aggiornata annualmente, anche in base a eventuali variazioni delle dotazioni tecnologiche e dei protocolli dell'Istituto.

Scopo della PUA
Scopo del presente documento è quello di informare e rendere responsabile l'utenza al fine di garantire un uso corretto e consapevole delle apparecchiature informatiche in dotazione e in uso all'interno dell'Istituto, nel rispetto della normativa vigente, definendo una linea di condotta precisa e chiara cui tutti gli utenti debbano attenersi.
È pertanto fondamentale conoscere le norme comportamentali e le procedure per l'utilizzo delle TIC in ambiente scolastico e avere la consapevolezza dei rischi cui si è esposti ogni volta che si naviga in Internet: esiste, infatti, la possibilità che durante il lavoro online si possa entrare accidentalmente in contatto con materiale inadeguato e/o illegale. Pertanto l'Istituto promuove l'adozione di strategie che limitino l'accesso a siti e/o applicazioni illeciti.

Stato di fatto: spazi fisici e virtuali disponibili nell'Istituto
- La quasi totalità delle aule del nostro Istituto, della Scuola Primaria e Secondaria, sono dotate di LIM, e la connessione alla rete della Scuola e quindi a Internet rientra nella pratica didattica quotidiana. I plessi di Scuola Primaria e l'edificio della Scuola Secondaria sono dotati di rete LAN con la connessione ad Internet, ed è attiva anche una rete wireless. I plessi dell'Infanzia attualmente non sono ancora collegati ad Internet.
- Il registro elettronico è in uso sia alla scuola secondaria sia alla scuola primaria.
- Gli uffici di segreteria, seguendo la normativa vigente, stanno perseguendo l'obiettivo della completa dematerializzazione; si presta particolare attenzione al potenziamento delle attrezzature informatiche, al mantenimento e costante aggiornamento della rete informatica e al potenziamento dei servizi digitali scuola-famiglia-studente.
- è una priorità il rinnovo dei PC nei laboratori, così che la scuola possa essere dotata di un numero adeguato di PC utilizzabili con gli alunni.
- I docenti devono servirsi delle TIC nelle attività didattiche in modo motivato e consono agli obiettivi educativi e didattici, assumendosi il fondamentale compito di responsabilizzare gli studenti, per renderli consapevoli sull'importanza della salvaguardia di un bene comune, grazie alle corrette norme di utilizzo.

Strategie dell'Istituto per garantire la sicurezza delle TIC
L'Istituto prevede le seguenti strategie per garantire la sicurezza in Rete:

- analizzare il fabbisogno formativo dei docenti e promuovere corsi di formazione inerenti all'uso sicuro e responsabile delle TIC e del web, sia nell' ambito privato, sia scolastico;
- attuare, eventualmente in collaborazione con esperti esterni, incontri per presentare le modalità corrette di fruizione del web (età minima per iscrizione ai social network), il problema della tutela dei minori su Internet e sui social network, le problematiche e i rischi legati a bullismo, cyberbullismo e uso non responsabile del web, a genitori, familiari e alle persone interessate presenti sul territorio;
- informare sulle problematiche psico-pedagogiche correlate all'uso della Rete;
-creare profili per diverse tipologie d'utenza;
- monitorare periodicamente il sistema informatico, in particolare per ciò che concerne l'uso di Internet, cronologia, cookie;
- chiedere, al bisogno, l'intervento delle società informatiche che si occupano di manutenzione e assistenza dei dispositivi con azioni in loco o da remoto;
- utilizzare penne USB, CD, DVD o altri dispositivi esterni personali solo se preventivamente autorizzati dal docente responsabile e sotto la sua vigilanza;
- organizzare un sistema di monitoraggio di eventuali problemi riscontrati durante l'uso delle TIC o della Rete e prevedere piani d'azione per risolvere i più frequenti;
- evidenziare il divieto di adottare comportamenti contrari al presente regolamento e alla normativa vigente come
    - scaricare file protetti da copyright e violare le leggi sui diritti d'autore;
    - visitare siti non inerenti all'attività didattica,
    - usare la Rete per interessi privati e personali;
    - alterare i parametri di protezione dei dispositivi utilizzati.

Nonostante l'Istituto si faccia carico di mettere in atto tutte le precauzioni necessarie per garantire agli studenti l'accesso a materiale appropriato, non è possibile evitare in modo assoluto che gli studenti incorrano in materiale indesiderato navigando su un computer dell'Istituto.
Gli studenti devono essere coscienti dei rischi cui si espongono quando sono in rete: devono essere educati a riconoscere ed evitare gli aspetti negativi di Internet come la pornografia, la violenza e il razzismo. Se venissero a contatto con materiali di questo tipo, devono sempre riferire l'indirizzo internet (URL) all'insegnante o al responsabile del laboratorio. Devono essere altresì informati sul rischio interno/esterno di scaricamento virus per mezzo di posta elettronica e/o operazioni di download eseguite tramite il browser.

Linee guida di buona condotta degli utenti
Ferme restando le strategie sistematiche messe in atto dall'Istituto di cui al precedente paragrafo e quanto eventualmente previsto nel Regolamento di Istituto, ciascun utente connesso alla Rete deve
- rispettare il presente regolamento e la legislazione vigente;
- tutelare la propria privacy, quella degli altri utenti adulti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni digitali cui ha accesso;
- rispettare la *netiquette*, ovvero quell'insieme di regole condivise che disciplinano il rapportarsi tra utenti della Rete, in contatto attraverso siti, forum, mail, blog, newsgroup…

Di seguito si dettagliano i comportamenti da tenere distinguendo attività e utenti.

Docenti
Durante l'attività didattica ogni docente può avvalersi degli strumenti a disposizione e deve:
- leggere, comprendere e aderire a questa policy;

- aver cura degli strumenti in dotazione, in particolare spegnendo correttamente tablet, PC, LIM e proiettori al termine del periodo di utilizzo o, in ogni caso, al termine delle lezioni ed eventualmente riponendoli nel luogo predisposto a cura del docente dell'ultima ora;
- accedere al registro elettronico attraverso il tablet o dal PC presente in classe e provvedere a compilare quanto di competenza, provvedendo successivamente al corretto logout;
- installare e utilizzare solo software autorizzati;
- non spostare i dispositivi dell'Istituto in locali diversi senza informarne il responsabile;
- non salvare sui dispositivi utilizzati file contenenti dati personali e/o sensibili;
- illustrare agli alunni le regole di utilizzo contenute nel del presente documento e informarli delle eventuali sanzioni disciplinari previste dal regolamento di Istituto;
- premurarsi che l'accesso degli alunni alla Rete avvenga sempre sotto la propria supervisione, informarli sui rischi cui sono potenzialmente esposti e sul corretto uso della Rete (motori di ricerca, piattaforme online, classi virtuali);
- guidare gli alunni nelle ricerche online: fornire obiettivi chiari, proporre indirizzi web, parole chiave per la ricerca, prediligendo siti istituzionali, creati ad hoc per la didattica; vigilare, durante la navigazione, che tutti usino in modo corretto la Rete, fornendo costanti indicazioni su ciò che è richiesto dalla *netiquette*;
- segnalare ai responsabili l'uso di siti internet non compatibili con la politica educativa dell'Istituto.

Studenti
Durante l'attività didattica gli alunni devono:
- leggere, comprendere e aderire a questa policy;
- accedere al laboratorio di informatica solo se accompagnati da docenti e seguire le indicazioni fornite in merito all'utilizzo delle TIC;
- accedere alla Rete solo in presenza e previa autorizzazione del docente responsabile dell'attività;
- utilizzare la strumentazione dell'Istituto solo per scopi didattici e non personali;
- lasciare immutata la configurazione di sistema dei dispositivi;
- sono previste eccezioni per l'uso dei dispositivi da parte degli alunni con BES, per i quali è possibile l'utilizzo del PC personale e la registrazione delle lezioni, regolamentati dai rispettivi PEI e PDP e dalla normativa vigente.
- Inoltre, per specifiche attività didattiche organizzate da un docente di classe, è consentito l'uso a scuola di dispositivi personali

Genitori
I genitori sono tenuti a
- leggere, aderire, comprendere e promuovere la PUA con i loro figli;
- controllare con regolarità il registro elettronico e il sito istituzionale dell'Istituto;
- confrontarsi con il personale dell'Istituto se dovessero sorgere preoccupazioni riguardo l'uso della tecnologia da parte del figlio

e sono invitati a
- monitorare il modo in cui i figli usano la tecnologia in ambiente extrascolastico e guidarli verso un comportamento responsabile e sicuro.

Altre tipologie di TIC
Lo studente non può utilizzare per scopi personali i device di sua proprietà nei locali scolastici e relative pertinenze. Durante l'orario scolastico agli studenti non è permesso l'uso della telefonia mobile. L'eventuale utilizzo di dispositivi personali durante una specifica

attività didattica, inserita nel PTOF, deve essere autorizzata e costantemente supervisionata dal docente di classe Le infrazioni e le sanzioni relative a un uso improprio delle TIC da parte degli studenti sono declinate nel Regolamento d'Istituto.

La *netiquette*

Chiunque si trovi a utilizzare le TIC, Internet e i servizi offerti dalla Rete deve attenersi a una serie di regole che disciplinano il comportamento degli utenti nel rapportarsi con gli altri; tali norme costituiscono la cosiddetta *netiquette*, una sorta di galateo della Rete.
Si riportano alcune delle norme su cui si intende sensibilizzare in modo particolare l'utenza:

- in Rete la comunicazione avviene principalmente attraverso testi, con conseguente rischio di essere fraintesi; talvolta, nei contesti opportuni, le emoticon possono aiutare a chiarire il tono del messaggio; risulta opportuno quotare i messaggi originari per facilitare la comprensione delle risposte;
- evitare di inviare messaggi ripetitivi, inutili o inopportuni (spam); evitare altresì l'invio di messaggi pubblicitari, "catene" o comunicazioni non espressamente richieste;
- in Rete si possono esprimere la propria opinione e le proprie idee, sempre rispettando tutti gli interlocutori e i fruitori del messaggio; la Rete offre la possibilità di entrare in contatto con milioni di utenti, dei quali vanno rispettati la nazionalità, la cultura, la religione, il sesso; non sono ammesse forme di razzismo o discriminatorie;
- è necessario rispettare gli interlocutori virtuali: i loro tempi nella risposta, che non andrà mai pretesa, il loro interesse o meno a quanto proposto; gli errori di digitazione, di grammatica o di sintassi non devono essere stigmatizzati, l'importante è che la trasmissione del messaggio avvenga con successo; si ricorda che lo scrivere in maiuscolo equivale a urlare: non abusarne;
- scegliere forum, social, community, chat, mailing list… cui si intende partecipare in base agli argomenti che interessano o alle esigenze emerse; partecipare rispettandone le regole e gli interventi dei moderatori;
- l'espressione del proprio parere deve avvenire in modo pacato, così da non provocare dure reazioni nelle persone con cui si comunica ed evitare "guerre di opinione";
- non utilizzare le proprie competenze digitali per violare siti o profili di altri utenti, pubblicare contenuti o conversazioni private, condividere fotografie, video o altri file di utenti terzi senza averne il consenso;
- curare la propria reputazione digitale, valutando sempre con la massima attenzione ciò che si vuole comunicare, pubblicare e condividere;
- rispettare la privacy degli altri utenti: ognuno può scegliere cosa pubblicare e cosa condividere delle informazioni che lo riguardano;
- evitare di rivelare dettagli, informazioni personali o dati sensibili propri o altrui;
- utilizzare la Rete con spirito critico: evitare di credere a tutto ciò che viene detto e diffidare di chi chiede informazioni personali o incontri dopo poco tempo che si è entrati in contatto perché non sempre è possibile avere la certezza dell'identità della persona con la quale si sta comunicando.

Comunicazione con l'Istituto

L'Istituto promuove una comunicazione chiara ed esplicita con il personale, le famiglie e il territorio, in particolare attraverso
- il sito istituzionale, costantemente aggiornato, che fornisce un'informazione puntuale e trasparente sulla documentazione e le attività relative all'Istituto;

- il registro elettronico, costantemente aggiornato dai docenti, sul quale le famiglie possono controllare assenze, voti, annotazioni (scuola secondaria) e schede di valutazione (scuola primaria e secondaria);
- la posta elettronica.

Garanzia e tutela della privacy
L'Istituto opera a ogni livello rispettando tutte le normative vigenti in merito alla tutela della privacy, come indicato sul sito istituzionale. La compilazione di un modello riguardante il trattamento immagini e audiovisivi degli alunni è richiesta
- a chi si iscrive per la prima volta nell'Istituto oppure all'ordine successivo attraverso la compilazione del modulo di iscrizione;
- a ciascun alunno all'inizio di ogni anno scolastico attraverso l'apposita modulistica presente sul sito istituzionale.

Sono permesse le riprese video e fotografiche di gite, saggi e recite scolastiche se destinate a un ambito familiare o amicale e non alla diffusione. Va, quindi, prestata grande attenzione all'eventuale pubblicazione delle medesime immagini su internet e in particolare sui social network. Per far questo, resta necessario, infatti, il consenso informato delle persone presenti nel video e nelle fotografie.
Gli esiti degli esami e degli scrutini finali sono pubblici ed esposti in forma cartacea: l'Istituto si impegna, però, ad evitare di fornire, anche indirettamente, informazioni sulle condizioni di salute degli alunni, o altri dati personali non pertinenti.

Sportello d'ascolto
Tra le misure di prevenzione che l'Istituto mette in atto per la prevenzione del disagio, anche per quanto riguarda l'uso delle TIC, di Internet e le relazioni virtuali che nella Rete si possono sviluppare, si registra la presenza alla scuola secondaria di Turbigo di uno "Sportello di ascolto", rivolto a tutti gli allievi, articolato in colloqui individuali e/o collettivi, con l'obiettivo di migliorare il benessere personale e scolastico di ogni singolo alunno, mediante un'attività di supporto della sfera emotiva, relazionale e comportamentale. È previsto, al suo interno, uno spazio riservato ai docenti e genitori al fine di individuare strategie efficaci per affrontare problematiche tipiche dell'età adolescenziale. L'Istituto si prodigherà nella tutela dei minori coinvolti, senza rendere in alcun modo identificabili, con dati o altri strumenti, gli stessi.

Didattica e azione dei docenti
L'Istituto, come evidenziato nel Piano Triennale dell'Offerta Formativa, pone particolare attenzione allo sviluppo della competenza digitale dei propri studenti, in linea con quanto previsto dal Piano Nazionale per la Scuola Digitale (PNSD). Questa competenza non può essere sciolta dalle competenze sociali e civiche che ogni alunno deve maturare, soprattutto per gli aspetti relazionali da esse implicati: l'ascolto, il rispetto reciproco, la capacità di vivere insieme. In tal modo ci si prefigge di prevenire eventuali fenomeni di disagio giovanile (bullismo, cyberbullismo, violenza, discriminazioni, uso di sostanze stupefacenti…). La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione (TSI) per il lavoro, il tempo libero e la comunicazione. Essa è supportata da abilità di base nelle TIC: l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni, nonché per comunicare e partecipare a reti collaborative tramite Internet. Si pone quindi enfasi sulla capacità di esplorare e affrontare in modo flessibile situazioni tecnologicamente nuove, adeguando le performance ai diversi contesti in cui si opera.

La competenza digitale è data dalla fusione delle dimensioni:

- etica, inerente alla responsabilità sociale, al sapere relazionarsi con gli altri utenti, al tenere dei comportamenti adeguati alle circostanze in cui ci si può imbattere e alla tutela della propria persona, per preservare la quale è necessario sapersi schermare dai possibili rischi;
- tecnologica, il saper individuare gli usi e i punti di forza dei dispositivi in uso e, quindi, scegliere i device e i mezzi adeguati per risolvere problemi;
- cognitiva, grazie alla quale è possibile saper leggere, selezionare e valutare dati, attraverso modelli astratti che conducano a un'analisi critica degli stessi al fine di individuare le informazioni attendibili e pertinenti al compito affidato tra tutte quelle offerte dalla Rete.

Per perseguire questi traguardi, i docenti adottano, come supporto alle attività scolastiche, le tecnologie educative e didattiche a disposizione, quali LIM, libri di testo digitali, risorse multimediali.
L'Istituto, coerentemente con quanto previsto dal PNSD, attiva dei percorsi di formazione rivolti ai docenti per acquisire le competenze necessarie.

Prevenzione, rilevazione e gestione dei casi
L'Istituto si prefigge come obiettivo quello di fornire a tutta l'utenza le competenze necessarie al fine di tenere comportamenti responsabili e corretti nella fruizione delle TIC e della Rete, così da poter prevenire i rischi in cui ci si può imbattere. Per quanto riguarda l'uso delle TIC, il personale in servizio presso l'Istituto, gli alunni e le loro famiglie sono informati e formati in merito alle modalità per utilizzare in modo sicuro, negli ambienti scolastici o all'esterno, i diversi device, quali tablet, PC, smartphone, fornendo loro indicazioni su come gestire impostazioni di cronologia, cookie, cache, firewall, malware e virus in genere.
Tutte le componenti scolastiche, in particolare personale docente e genitori, devono essere formate, informate e aggiornate sui fenomeni del bullismo e del cyberbullismo.
A tal fine, presso il nostro istituto sono stati svolti negli ultimi anni percorsi formativi sull'argomento e ed è stato nominato un referente di istituto sul tema del bullismo e del cyberbullismo, attivo con una Commissione.
L'Istituto si impegna a formare e aggiornare i docenti sulle modalità e gli indicatori per riconoscere eventuali casi o situazioni a rischio e sulle procedure da seguire
Per ulteriori informazioni si rimanda all'omonimo paragrafo all'interno dell'Epolicy di Istituto.

Diffusione della PUA
La PUA e le regole in essa contenute verranno approvate dal Collegio dei Docenti e dal Consiglio di Istituto e pubblicate online sul sito istituzionale dell'Istituto.
Il personale scolastico è tenuto alla lettura e sottoscrizione della PUA, nonché allo sviluppo delle linee guida e all'applicazione scrupolosa delle istruzioni sull'uso sicuro e responsabile della Rete.
Gli studenti sono informati dei contenuti della PUA attraverso il Patto di Corresponsabilità e costantemente supportati per un uso responsabile e consapevole delle TIC e della Rete.
Gli studenti e i loro genitori/tutori devono firmare il documento.
I genitori o i tutori sono invitati a prestare la massima attenzione ai principi e alle regole contenuti in questo documento; si richiede un impegno costante affinché siano rispettate anche in ambito extrascolastico, assistendo i minori nel momento dell'utilizzo della Rete e adottando tutti i sistemi di sicurezza per diminuire i possibili rischi della Rete.

Sottoscrizione PUA
Si rimanda al modello della pagina successiva.

Informazione genitori

Consenso dei genitori/tutori dell'allievo/a .....……. per l'*accesso a Internet* nell'IC Valdagno 1, iscritto alla primaria di …… / Secondaria di primo grado.

Ho letto la Politica d'Uso Accettabile e responsabile di Internet e consento a mio figlio/a di utilizzare l'accesso ad Internet a scuola.

Sono cosciente che l'Istituto prenderà tutte le precauzioni per garantire che gli studenti non abbiano l'accesso a materiale non adeguato.

Sono consapevole che l'Istituto non può essere responsabile per la natura o il contenuto del materiale reperito su Internet e non responsabile degli eventuali danni provocati.

Data..... Firma.....

Liberatoria

Consenso dei genitori/tutori dell'allievo/a …….…… per la *pubblicazione su Internet dei lavori/ fotografie* del proprio/a figlio/a, iscritto iscritto alla primaria di …… / Secondaria di primo grado.

Il sottoscritto acconsente che siano *pubblicati su Internet lavori realizzati* dal proprio figlio/a.

Acconsente altresì che siano *pubblicate le fotografie del proprio figlio/a ma che, secondo le regole dell'Istituto, non lo identifichino chiaramente e che non venga inserito il nome* per intero.

Data..... Firma.....

Contratto dello studente

Cognome e nome dell'alunno/a .....……..... iscritto alla primaria di …… / Secondaria di primo grado.

Ho compreso le regole della Politica d'uso accettabile e responsabile di Internet fissate dall'Istituto.

Utilizzerò il sistema informatico e Internet in modo responsabile e seguirò le sopra citate regole.

Sono consapevole che se violerò queste regole l'Istituto potrò essere sottoposto alle sanzioni disciplinari previste dall'Istituto in materia.

Data..... Firma.....