REPUBBLICA ITALIANA

ISTITUTO COMPRENSIVO "BASSA ANAUNIA-TUENNO"
Istituto comprensivo di scuola elementare e media
Via Colle Verde, 3 - 38010 DENNO
Cod. Fisc. 96056980228 - ☏ 0461 655783 🖷 0461 655066
www.icbassaanauniatuenno.it
e-mail: segr.ic.denno@scuole.provincia.tn.it
PEC: ic.bassaanaunia@pec.provincia.tn.it

PROVINCIA AUTONOMA di TRENTO

REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI

Versione ottobre 2020

Approvato dal consiglio dell'istituzione scolastica il 5 novembre 2020 delibera n. 29

REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI

Versione ottobre 2020

L'Istituto Comprensivo di scuola elementare e media di Bassa Anaunia-Tuenno mette a disposizione dei propri alunni e di altri soggetti autorizzati una serie di strumenti informatici (PC, rete, connessione ad internet, ecc.) per consentire la soddisfazione di esigenze connesse alla ricerca e alla didattica.

Il Dirigente Scolastico intende di conseguenza definire le modalità d'uso dei predetti strumenti informatici nel giusto contemperamento dei diritti dei soggetti coinvolti con l'osservanza delle disposizioni in materia di trattamento dati personali e sicurezza informatica.

Ai sensi del Regolamento UE 679/2016e del D.lgs. 101/2018 l'utilizzo di sistemi informatici o telematici deve infatti avvenire attraverso la massima cautela e in osservanza delle disposizioni vigenti in materia di protezione dei dati personali.

* *

1. L'utilizzo di tutti gli strumenti informatici di proprietà dell'istituto deve avvenire osservando scrupolosamente le regole di buona diligenza e prudenza, con senso di responsabilità e seguendo le istruzioni impartite dalla Direzione, dai docenti e dalle persone da essi delegate.

2. L'uso degli strumenti (*PC, attrezzatura informatica e aule didattiche, notebook, rete, ecc*.) è consentito unicamente agli utenti autorizzati dalla Direzione ovvero dai responsabili della gestione della struttura informatica.

3. L'accesso agli strumenti è consentito solo previa autenticazione personale effettuata mediante sistema di identificazione (attribuzione individuale di nome utente e password). Le politiche di gestione delle password dovranno rispettare il dettato normativo in materia di privacy e sicurezza informatica.
4. In ogni caso, ciascun utente è personalmente responsabile per l'uso del proprio account ed è tenuto a tutelarlo da accessi non autorizzati. Non è di conseguenza ammessa la comunicazione del proprio account a terzi.

5. Le disposizioni di seguito riportate, relative alle credenziali di autenticazione, contribuiranno a garantire la sicurezza nell'accesso:

    a. *Ogni utente è tenuto a scegliere una password composta da almeno 8 caratteri alfanumerici, che non contenga riferimenti che riconducano agevolmente all'incaricato (es: non inserire nome o cognome proprio e di familiari).*

    b. *La password è personale, riservata e non può essere ceduta o comunicata ad alcuno. È pertanto vietato l'uso della password di altri utenti; qualora se ne venisse a conoscenza è obbligatorio segnalare il fatto all'utente interessato, al docente responsabile e all'amministratore.*

    c. *E' obbligatorio modificare la password ogni volta che il sistema ne faccia richiesta.*

    d. *Per esigenze operative o di sicurezza e integrità del sistema e dei dati, l'amministratore di sistema ha facoltà di modificare la password degli utenti.*

6. Qualsiasi attività svolta utilizzando l'account attribuito sarà ricondotta nella sfera di responsabilità dell'utente assegnatario del codice. Si segnala che ogni utente è civilmente responsabile per i danni cagionati all'Istituto, all'Internet Provider e/o a terzi, non solo in relazione ai propri fatti illeciti ma anche per quelli commessi da chiunque utilizzi il suo codice utente e password.

7. L'uso dei PC ubicati nelle aule e nei laboratori e dei relativi programmi, compatibilmente con i fini didattici, deve preferibilmente avvenire in modo tale da non salvare in cartelle condivise dati personali e riservati, se non per fini strettamente necessari.

8. L'accesso alla rete internet mediante le strutture informatiche dell'Istituto deve essere finalizzato al perseguimento di fini connessi all'attività didattica e di ricerca.

9. Non è consentito accedere ed utilizzare la rete internet in modo difforme da quanto previsto dal presente disciplinare e, ovviamente, dalle leggi penali, civili ed amministrative in materia. In ogni caso, ogni utente è direttamente responsabile dell'uso del servizio di accesso ad Internet, dei siti ai quali accede, delle informazioni che immette e riceve.

10. Qualora un utente dovesse riscontrare malfunzionamenti, guasti o situazioni di rischio per la sicurezza o l'integrità del sistema causati da comportamento doloso o

comunque non conforme alle istruzioni e disposizioni è tenuto a darne immediata comunicazione ad un docente responsabile.

E' severamente vietato:

1. *Utilizzare le attrezzature informatiche messe a disposizione degli utenti per scopi diversi da quelli afferenti fini connessi alla didattica e la ricerca.*
2. *Svolgere operazioni di loading (caricamento) e downloading (scaricamento) non autorizzate o non rientranti nei fini predetti.*
3. *Salvare in cartelle condivise file contenenti dati personali o informazioni riservate.*
4. *Modificare le configurazioni dei PC ubicati nella sede dell'Istituto.*

11. Il personale docente e i tecnici informatici sono tenuti a vigilare sul corretto utilizzo delle attrezzature informatiche ed hanno il dovere di informare senza ritardo la Direzione sull'eventuale utilizzo improprio dei sistemi, dei PC e dei relativi programmi.

12. Nel caso in cui si ravvisasse un utilizzo improprio delle predette attrezzature, la Direzione si riserva ogni idoneo provvedimento in linea con le politiche di gestione elaborate nel presente regolamento, tra cui:
    - poter controllare gli accessi alle strutture, ivi compreso il corretto utilizzo di elaboratori, programmi e sistemi operativi, in linea con le presenti regole di utilizzo e nel rispetto delle disposizioni vigenti in materia di protezione dei dati personali;
    - poter procedere alla rimozione di ogni file estraneo pericoloso per la sicurezza del sistema, non attinente all'attività didattica o acquisito ed installato in violazione di principi generali di buona condotta o delle norme in materia di copyright e diritto d'autore.
    - adottare un sistema generale di controllo e prevenzione sugli accessi alla rete e di limitazione all'uso della stessa, anche tramite il divieto di navigazione su determinati siti (mediante accessi limitati e filtri per categorie di utenti);
    - implementare costantemente le misure di sicurezza previste dal reg. UE 679/2016

- sospendere, anche selettivamente, il servizio di accesso ad Internet nei seguenti casi:
    i. esigenze di manutenzione;
    ii. accertamento di un uso non corretto del servizio da parte dell'utente;
    iii. in caso di manomissioni e/o interventi su hardware/software;
    iv. diffusione o comunicazione imputabili direttamente o indirettamente all'utente relativamente a profili d'accesso o altre informazioni riservate; accesso a directory/file/siti non rientranti fra quelli per cui l'utente abbia autorizzazione.

LINEE GUIDA PER L'USO CORRETTO DELLA RETE E DELLE AULE DIDATTICHE DELL'ISTITUTO

1. Sul web gli studenti non devono di norma rivelare i propri dati personali (nome, cognome, indirizzo, numero di telefono personale, ecc.).

2. Gli studenti non possono relazionare autonomamente con altri soggetti (chat, social network, ecc.) senza il permesso degli insegnanti di riferimento. Ogni comportamento difforme rientrerà nella sfera della diretta responsabilità dell'utente.

3. Senza diversa autorizzazione è permesso solo l'accesso ai collegamenti consentiti mediante l'impostazione del sistema di autenticazione.

4. Agli studenti di norma non è permesso accedere a newsgroup e chat room.

5. L'accesso ad Internet può essere filtrato attraverso un proxy server che scherma alla fonte i siti inidonei – questo servizio può essere disabilitato solo dall'amministratore di sistema.

6. Ciò premesso, l'Ente può avvalersi di sistemi controllo relativi al corretto utilizzo degli strumenti indicati: tali controlli saranno effettuati qualora le misure preventivamente esposte non siano state sufficienti per evitare comportamenti anomali. I controlli saranno svolti con gradualità, secondo i principi di pertinenza e non eccedenza. In seguito si espongono le modalità di tali controlli:

7. In prima battuta si effettuerà un controllo preliminare su dati anonimi ed aggregati; si procederà pertanto con verifiche di rete o gruppo.

8. Il controllo anonimo può terminare con un avviso di rilevazione di un utilizzo inadeguato degli strumenti indicati; contestualmente si diramerà una nota di richiamo invitando gli utenti ad attenersi alle regole elaborate.

9. Se si dovesse ripetere l'anomalia, sarà facoltà dell'Ente procedere con controlli più mirati, anche su base individuale ed assumere ogni idoneo e conseguente provvedimento.

10. I dati contenuti nei file di log, relativi agli accessi ad Internet e al traffico telematico, possono essere conservati per il tempo strettamente necessario al perseguimento di finalità organizzative e di sicurezza. I file di log potranno essere utilizzati in tali casi:

11. Produzione di report statistici che presentino i dati relativi alla navigazione in forma aggregata e anonima.

12. Analisi dei problemi riscontrati nel sistema e soluzione dei medesimi, estraendo i dati in modo aggregato e in forma anonima