ISTITUTO COMPRENSIVO STATALE
C.B. CAVOUR
Via Carbone 6 – 95129 Catania – tel /fax 0953104480
www.scuolacavourcatania.edu.it - ctic8a700p@istruzione.it - ctic8a700p@pec istruzione.it

POLICY DI SICUREZZA IT PER GLI ALUNNI

1. Campo d'applicazione, scopo e destinatari

Lo scopo di questo documento è definire delle chiare regole per l'uso del Sistema Informativo e di altre risorse informatiche all'interno dell'Istituto.
Destinatari di questo documento sono tutti gli alunni dell'Istituto Comprensivo Statale "C.B. Cavour", che sono stati autorizzati o saranno autorizzati all' uso del Sistema Informativo aziendale, per lo svolgimento di attività didattiche.

2. Regole di Sicurezza di Base

2.1. Definizioni

Sistema informativo: include tutti i server e i client, l'infrastruttura di rete, il software di sistema e applicativo, i dati e altri sottosistemi e componenti di computer che sono di proprietà o utilizzati all'organizzazione o che sono sotto la responsabilità dell'organizzazione. L'uso di un sistema informativo include anche l'uso di tutti i servizi interni o esterni, come l'accesso a Internet, l'email, ecc.
Risorse informative: nel contesto di questa politica, il termine *risorsa informativa* viene applicato ai sistemidi informazione e ad altre informazioni / attrezzature inclusi documenti cartacei, telefoni cellulari, computer portatili, supporti di memorizzazione di dati, ecc**.**
S.I.: Funzione Aziendale Sistemi Informativi

2.2. Utilizzo accettabile

Le risorse informative possono essere utilizzate dall'alunno solo per esigenze didattiche.

2.3. Attività vietate

È vietato utilizzare le risorse informative in modo da occupare inutilmente capacità, indebolire le prestazioni del sistema informativo o rappresentare una minaccia alla sicurezza. È inoltre vietato:

- scaricare file di immagini o video che non hanno uno scopo legato all'attività didattica, inviare catene di e-mail, giocare, ecc
- installare software su un computer locale senza autorizzazione esplicita.
- utilizzare applicazioni Java, controlli Active X e altri codici mobili, tranne se autorizzato da S.I..
- utilizzare strumenti crittografici (cifratura) non autorizzati su un computer locale.
- scaricare il codice del programma da un supporto esterno
- installare o utilizzare dispositivi periferici quali modem, schede di memoria o altri dispositivi per la memorizzazione e la lettura di dati (ad esempio unità flash USB) senza autorizzazione esplicita di S.I..

2.4. Portare delle risorse fuori dal sito

Apparecchiature, informazioni o software, indipendentemente dalla forma o supporto di memorizzazione, non possono essere portati fuori dal sito senza previa autorizzazione scritta da parte della Direzione dell'Istituto.
Finché tali beni sono al di fuori dell'organizzazione, devono essere controllati dalla persona a cui è stata concessa l'autorizzazione.

2.5. Autorizzazioni per l'uso del sistema informativo

Gli alunni (utenti del sistema informativo) possono accedere solo a quelle risorse del sistema informativo per le quali sono state esplicitamente autorizzati.
Gli alunni possono utilizzare il sistema informativo solo per gli scopi per i quali sono stati autorizzati, ovvero per i quali hanno ottenuto i diritti di accesso.
Gli alunni non devono prendere parte ad attività che possono essere utilizzate per aggirare i controlli di sicurezza del sistema di informazione.

2.6. Responsabilità dell'account utente

L'alunno non deve, direttamente o indirettamente, consentire a un'altra persona di utilizzare i suoi diritti di accesso, cioè il nome utente e password, e non deve utilizzare il nome utente e / o la password di un'altra persona. L'uso di nomi utente di gruppo è vietato.
Il proprietario dell'account utente è il suo utente (alunno), che è responsabile del suo utilizzo e di tutte le transazioni eseguite attraverso questo account utente.

2.7. Responsabilità relative alla password

Ad ogni alunno verrà consegnata una password per l’accesso al Sistema Informatico. Gli alunni devono applicare buone pratiche di sicurezza quando usano le password:

- le password non devono essere divulgate ad altre persone, inclusi gli amministratori di gestione e di sistema
- le password non devono essere trascritte, a meno che un metodo sicuro sia stato approvato dalla Direzione dell’Istituto.
- le password devono essere cambiate se vi sono indicazioni che le password o il sistema potrebbero essere stati compromessi. in tal caso deve essere segnalato un incidente di sicurezza alla Direzione dell’Istituto che provvederà alla creazione ed alla consegna di una nuova password.
- Le password consegnate avranno le seguenti caratteristiche:
    - Lunghezza almeno otto caratteri
    - utilizzando almeno un carattere numerico
    - utilizzando almeno un carattere alfabetico maiuscolo e almeno uno minuscolo
- le password non devono essere memorizzate in un sistema di accesso automatico (ad esempio macro o browser)

2.8. Uso di Internet

È possibile accedere a Internet solo attraverso la rete wifi dell'Istituto con una infrastruttura adeguata e una protezione firewall. È vietato l'accesso diretto personale a Internet tramite modem, Internet mobile, o altri dispositivi per l'accesso diretto a Internet.
Internet, e la relativa navigazione, deve essere considerato uno strumento didattico, pertanto l'alunno è responsabile di tutte le possibili conseguenze derivanti dall'uso non autorizzato o inappropriato di servizi o contenuti Internet.

Confermo di aver ricevuto:

- Copia della Policy
- Credenziali di accesso (utente e password)

Data _____ Firma Genitoriale