Ministero dell'Istruzione
LICEO GINNASIO STATALE "DANIELE MANIN"
Via Cavallotti, 2 - 26100 Cremona
TEL. 0372/21545 – FAX 0372/20092 C.F. 80003300193
Sito: www.liceomanin-cr.gov.it
e-mail: crpc02000a@istruzione.it – PEC: crpc02000a@pec.istruzione.it

Sistema di Gestione Qualità UNI EN ISO 9001 Certificato (EA37)

Ai Docenti
All'Ufficio di segreteriaAl personale ATA
Agli alunni e ai loro genitori
DUE SEDI

Oggetto: Misure minime di sicurezza informatica

La più recente normativa in materia di Sicurezza Informatica, e in particolare la Circolare 18 aprile 2017, n. 2/2017 – Agenzia per l'Italia Digitale, impone alle scuole l'implementazione di alcune misure minime di sicurezza. Si richiede pertanto la collaborazione di tutta l'utenza affinché tali misure siano applicate in modo efficace.

Il crescente diffondersi di malware (virus e altro) espone in modo sempre più preoccupante i dispositivi e le reti a possibili attacchi ed infezioni dalle conseguenze dannose sia per il funzionamento delle dotazioni informatiche che per la protezione dei dati gestiti.

Per questo motivo si richiamano gli utenti ad un attento e consapevole utilizzo dei dispositivi ed in particolare di quelli messi a disposizione della scuola, nonché al rispetto delle seguenti misure minime di sicurezza:

1. Rispetto dei Regolamenti di istituto in materia di utilizzo delle tecnologie informatiche:

- Tutti gli utenti sono tenuti ad un'attenta lettura e al rispetto dei Regolamenti di istituto relativi all'utilizzo degli strumenti tecnologici già emanati e che saranno di volta in volta pubblicati a seguito dell'ampliamento della dotazione tecnologica di istituto.

2. Utilizzo della posta elettronica:

Poiché una delle maggiori fonti di contagio è costituita dalla posta elettronica, si dispone quanto segue:

- a partire dal 14 febbraio 2018 tutti gli utenti sono tenuti ad utilizzare esclusivamente l'indirizzo mail d'istituto con dominio @liceomanin-cr.gov.it per tutte le comunicazioni scolastiche; nel frattempo, i docenti, già in possesso delle credenziali di accesso all'account Google di istituto, sono caldamente invitati a preferire l'utilizzo di questo account rispetto a quello personale (al fine di evitare confusione, poiché gli indirizzi dei destinatari sono spesso memorizzati automaticamente, si raccomanda di non inviare mail da un account personale ad un account di istituto o viceversa; si suggerisce anche di utilizzare l'account di istituto per le comunicazioni di tipo scolastico con enti esterni); gli alunni delle classi del biennio che hanno già svolto la formazione Google con le Prof. Marzani e Bergamaschi sono, allo stesso modo, invitati ad utilizzare fin d'ora l'account di istituto; le altre classi potranno utilizzare gli account di istituto non appena svolta la formazione (classi del biennio) o una volta ricevute le credenziali (classi del triennio); si ricorda che, per motivi di sicurezza, al momento gli alunni possono comunicare tramite l'account di istituto solo con altri utenti del dominio della scuola;
- l'uso della propria posta privata per motivi che esulano dall'attività scolastica su dispositivi della scuola non è consentito, fatti salvi motivi di necessità e urgenza che dovranno essere motivati alla direzione dell'Istituto; l'accesso può avvenire solo tramite web mail e le operazioni consentite riguardano l'invio e la visualizzazione dei messaggi, escludendone il download sui dispositivi dell'istituto.

3. Utilizzo di chiavette Usb e scambio di file:

- Poiché anche le chiavette Usb possono essere mezzi di contagio, si raccomanda di limitarne il più possibile l'uso sui Pc della scuola e di effettuarne preliminarmente una scansione, così come richiesto automaticamente dall'antivirus;

- al fine di limitare l'utilizzo di chiavette Usb, si suggerisce di optare per il salvataggio dei file sui cloud di istituto (Google Drive o OneDrive);
- poiché la trasmissione di file infetti è veicolo di contagio, si suggerisce di limitare il più possibile il passaggio di file modificabili fra utenti e di preferire l'archiviazione e la modifica dei file in modo condiviso su Google Drive.

4. Utilizzo degli account d'istituto:

A tutela della riservatezza dei dati, tutti gli utenti sono tenuti alla massima attenzione nell'uso delle credenziali di accesso al registro elettronico e agli account di istituto; si raccomanda pertanto di:

- utilizzare password che abbiano un minimo di complessità (almeno 8 caratteri alfanumerici fra cui almeno unnumero e una lettera maiuscola);
- cambiare la password con una certa frequenza (almeno ogni 90 giorni in presenza di dati sensibili);
- cambiare immediatamente la password nel caso di sospetto di accesso di terzi al proprio account o difurto/smarrimento del proprio dispositivo;
- non memorizzare le proprie password sui PC dell'istituto;
- non divulgare le proprie password e custodirle in modo sicuro;
- uscire dal proprio account al termine della sessione di lavoro su un dispositivo utilizzato anche da altri utenti.

5. Utilizzo dei Pc dell'istituto:

- A tutela della riservatezza dei dati, sui PC dell'istituto destinati all'utilizzo di più utenti non devono permanere documenti privati ed in particolare quelli contenenti dati personali, dati riservati o sensibili relativi ad alunni o personale della scuola.

6. Navigazione in Internet sui Pc dell'istituto:

Al fine di evitare la diffusione di virus, malware, adware … sui Pc di istituto, si raccomanda di:

- non navigare su siti non sicuri;
- non scaricare applicazioni o file di dubbia provenienza;
- evitare di navigare sui social network (Facebook o altro), se non strettamente necessario per motivi scolastici.

Si ricorda che comportamenti difformi rispetto a quelli qui raccomandati determinano responsabilità personali pereventuali danni a persone e/o cose; in tal caso, nessuna responsabilità può essere imputata all'istituzione scolastica.

Si allegano alla presente, raccomandandone un'attenta lettura:

- una breve guida sui malware più diffusi e su alcune semplici regole per potersi difendere evitando o comunque diminuendo sensibilmente i pericoli di infezione;
- la guida redatta dal Garante per le scuole per una corretta individuazione e gestione dei dati personali e sensibili.

Per qualsiasi chiarimento, è possibile rivolgersi al Dirigente Scolastico o all'Animatore Digitale.

Si ringrazia anticipatamente per la collaborazione.

IL DIRIGENTE SCOLASTICO
Mirelva Mondini*
**Firma autografa apposta sull'originale e sostituita dall'indicazione a stampa del soggetto responsabile ex art. 3, co.2 del D.Lgs. 39/93*