ISTRUZIONI DI BASE PER PRESERVARE LA SICUREZZA DEI DATI A SCUOLA

I. C. Iva Pacetti Prato

a.s. 2023/2024

Introduzione:

- Ad ogni membro del personale viene fornito fino dalla prima presa di servizio **un account personale di servizio** con dominio @pacettiprato.edu.it facente parte della piattaforma **Google Workspace** di istituto. Le app accessibili (Gmail, Drive, Meet ecc…) sono uno strumento di lavoro e pertanto devono essere utilizzate solo per usi professionali.
- La stessa cosa vale per l'accesso all'altra piattaforma online in uso nella scuola: **Microsoft Office 365** (app Onedrive, Teams ecc…)
- Per le **regole** di uso delle piattaforme si veda il Regolamento Uso Piattaforme **Google Workplace** e **Microsoft Office365** .
- Le persone assegnatarie dell'**account di accesso alle piattaforme Google Workspace e Microsoft Office 365** sono responsabili del corretto utilizzo delle stesse.

1. ACCESSO AI PC DI CLASSE, MONITOR E LORO UTILIZZO
2. EMAIL E ALTRE APP PIATTAFORME GOOGLE E OFFICE365
3. SALVATAGGIO DATI
4. PASSWORD
5. DIDATTICA DIGITALE INTEGRATA

ACCESSO AI PC DI CLASSE, MONITOR E LORO UTILIZZO

- Si può accedere ai PC della scuola solo con un **proprio account**. Ogni PC è dotato di un **account Amministratore** (accessibile appunto solo all'Amministratore), di **tanti account utente** quanti sono i docenti della classe che utilizzano quel PC e uno **ospite** per i docenti che effettuano una supplenza sulla classe. In particolare per questo caso si ricorda che al termine di una sessione occorre disconnettersi dall'account di posta Gmail e riconnettersi solo dal proprio: avvertire un collega che abbia lasciato l'account aperto (e disconnetterlo). La stessa istruzione vale anche, e a maggior ragione, per la disconnessione da Google Drive, Microsoft One Drive e dal Registro Elettronico)

- Nel caso si debba **lasciare** l'aula:
  - occorre prima **disconnettere** l'account (dal pulsante "Start" – Nome utente – Disconnetti) o attivare la funzione **sospensione** (dal pulsante "Start"-Arresta-Sospendi).
  - Non lasciare **mai** il Registro Elettronico aperto.

- Non è consentito agli utenti **installare** programmi se non previa autorizzazione dell'Amministratore. E' vietato lo **scaricamento** di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dall'Amministratore.

- E' vietata la **navigazione** in Internet con dispositivi della scuola per motivi diversi da quelli legati all'attività lavorativa stessa.

- I PC portatili non devono essere lasciati **incustoditi** e riposti in un luogo sicuro. I cavi delle varie strumentazioni devono essere inseriti e scollegati in modo **scrupoloso**.

- Per l'utilizzo dei **Monitor touch**, di nuova generazione:
  - Non archiviare i **dati**.
  - Utilizzare il **browser** integrato senza inserire il proprio account, se necessario occorre ricordarsi sempre di disconnettersi.
  - Se si collega un **pc personale** utilizzare l'apposito cavo in dotazione alla classe collegandolo alla porta frontale.
  - Alla fine della giornata **spengere** il dispositivo e poi l'interruttore **generale**.

- Saranno disponibili nei plessi Santa Gonda e Dalla Chiesa dei computer portatili "**jolly**", da poter utilizzare in caso di malfunzionamenti del pc della classe. Per ogni problematica tecnica scrivere a:

referente.tecnico@pacettiprato.edu.it

EMAIL E ALTRE APP PIATTAFORME GOOGLE E OFFICE365:

- Quando si invia un'email assicurarsi **dell'esattezza del destinatario**, soprattutto quando si inviano informazioni o allegati con dati che sono soggetti a protezione.

- Nel caso si debbano inviare email a utenti esterni, assicurarsi che i dati divulgati non siano **soggetti a protezione**. Per questo si vedano le disposizioni richiamate nella formazione sulla Privacy di novembre.
  - Per inviare un messaggio a diversi utenti senza divulgarne agli altri l'indirizzo fare uso della funzione **CCN** (conoscenza nascosta): in questo modo ciascuno potrà vedere solo sé stesso come destinatario del messaggio.

- Nel caso di **mittenti sconosciuti** o messaggi **insoliti**, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprirli.

- **Non aprire allegati** sospetti, soprattutto in formato exe, zip.

- Non **immettere** mai dati personali (meno che mai sensibili o, ad esempio, di tipo bancario) su moduli aperti in base a richieste ricevute per email.

- Diffidare di email scritte con **errori** in italiano.

SALVATAGGIO DATI

- **Evitare di salvare** documenti sul PC, in particolare sul desktop, ma anche in altre cartelle. I file eventualmente salvati nelle cartelle del PC non devono contenere dati non soggetti a divulgazione (dati sensibili alunni, verbali, voti, giudizi ecc…) e comunque non devono essere accessibili ad altri utenti. Eliminare i file relativi a scannerizzazioni subito dopo averli utilizzati.
- Svuotare regolarmente la cartella Download e il Cestino (di Windows)

- **Per il salvataggio** utilizzare cloud (One Drive permette di utilizzare anche una versione semplificata ma perfettamente funzionante di Office, garantendo la piena compatibilità: altrimenti utilizzare Drive e le app di Google). Si consiglia di organizzare i documenti in cartelle tematiche per facilitare la ricerca dei file archiviati.

- Si dovrà **evitare di utilizzare chiavette USB**, le quali fra l'altro sono spesso veicolo di virus. In ogni caso, qualora le si utilizzassero per archiviare e trasportare dati soggetti a protezione, si dovrà **utilizzare una chiavetta dotata di sistema di sicurezza** (impronta digitale, codice di accesso o altri dispositivi di criptazione)

PASSWORD

- **Proteggere** gli accessi a Google Workspace e Office 365 con robuste password: almeno 8 caratteri fra i quali una maiuscola, una minuscola, un numero e possibilmente un carattere speciale
- **Cambiare** frequentemente le password
- Evitare di utilizzare la **solita** password per più accessi diversi
- **Segnarsi** le password in un luogo sicuro: esistono anche degli appositi programmi gratuiti (es. Keepass), ma ci se le può segnare, ad esempio, sul cellulare (anche qui esistono delle app che svolgono questa funzione) o sull'agenda cartacea. In ogni caso le password personali devono essere custodite con la massima cautela non devono essere rese accessibili ad altri.
- **Non salvare le password in automatico** su computer accessibili anche ad altri utenti (quali sono tipicamente quelli di scuola).
- Non utilizzare la funzione di **sincronizzazione** dell'account su browser (Es. Chrome); se inavvertitamente si fosse attivata la sincronizzazione la si deve disattivare.
- I **documenti** eventualmente **condivisi** su cartelle **online che contengano dati particolari** devono essere pseudonimizzati o anonimizzati in modo da non rendere possibile il riconoscimento delle persone coinvolte a chi non ne abbia il diritto