NORME DI COMPORTAMENTO DA TENERE PER LA FORMAZIONE A DISTANZA – DOCENTI

Di seguito alcune buone regole per il corretto trattamento dei dati e le forme di protezioni da seguire sugli strumenti elettronici personali o dati in uso dall'Istituto, nella formazione a distanza.

Premessa

- Prima di iniziare le lezioni è importante controllare la stabilità e la potenza della connessione Internet per non rischiare di perdere il segnale e quindi non impartire parti importanti della formazione.
- Controllare che lo strumento elettronico (personal computer, notebook, etc.) sia munito di un microfono e/o in caso di video lezioni di una webcam
- Controllare che il dispositivo elettronico che si sta utilizzando abbia il sistema operativo aggiornato
- Verificare che gli strumenti elettronici che si utilizzano siano protetti da password, utilizzando i criteri elencati di seguito a titolo esemplificativo:
  - comporla utilizzando almeno 8 caratteri, alfanumerici, con alternanza di maiuscole e minuscole e, ove possibile, simboli;
  - non basare la scelta su informazioni facilmente deducibili quali, ad esempio, il proprio nome, il nome dei propri familiari, le date di nascita, etc.;
  - mantenerla riservata, evitando di divulgarla o di trascriverla su supporti cartacei o di memorizzarla sul proprio pc o altro strumento accessibile a soggetti terzi;
  - non memorizzare sul browser le credenziali di accesso;
- Dopo un lasso di tempo prestabilito di inattività del PC, deve attivarsi automaticamente uno screen-saver o protezione di sessione e impostare la riapertura della schermata con l'inserimento della password.

Backup file/dati

Se si generano file e/o dati inerenti l'attività della didattica a distanza, si ricorda che, le postazioni dei singoli personal computer utilizzati, non sono sottoposti a backup automatico di alcun tipo. Perciò in conformità con quanto stabilito dal GDPR 2016/679, su tutti i dati, dovranno essere effettuati dei back up su apposito supporto esterno con frequenza ciclica. I supporti su cui effettuare il back up dovrà essere concordato con il titolare del trattamento (ad es.: Usb, CD, Hard Disk, etc).

Principi da rispettare

- Datti degli orari precisi in cui gestire l'attività assegnata;
- Uno spazio da lavoro è d'obbligo, la cosa migliore è avere una stanza apposta in cui trascorrere le ore da dedicare all'attività da svolgere, così da poter gestire il tutto in piena tranquillità ed avere tutto ciò che serve a portata di mano. Questa location oltre ad essere tranquilla deve essere anche ben ordinata, perché il disordine sul lavoro non aiuta mai e sopratutto non aiuta circondarsi di oggetti o cose che non ci servono per lavorare, quindi cerca di fare una sorta di decluttering sul tuo angolo da lavoro;
- Il lavoro va pianificato, quindi avere un piano di lavoro ben preciso da seguire, perché questo è fondamentale per terminare ogni lavoro in tempo senza alcun stress;
- Un po' di relax non deve mancare anche se ti ritrovi con troppo lavoro trova lo stesso il tempo per una pausa, anche piccola, per poter staccare la testa dal lavoro, magari datti anche per la pausa un orario ben preciso da rispettare;
- Non accumulare arretrati e/o lavorare con anticipo;
- Evitare il più possibile le distrazioni web. Come? Silenziando o bloccando alcune app, anche attraverso alcuni tool che ne limitano l'utilizzo;
- Disponi dei dati e tienine cura come il buon padre di famiglia;
- I documenti contenenti dati personali, devono essere custoditi in modo da non essere accessibili;

- I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro, se possibile dedica un arredo alla conservazione dei documenti;
- Si deve limitare all'indispensabile la duplicazione (fotocopie, ecc) di documenti contenti dati personali, e non riutilizzare mai le fotocopie di documenti contenti dati personali come carta riciclata.

Consigli per la formazione su app diverse dal registro elettronico

- Non accedere alle app attraverso il proprio profilo social (ad es.: Facebook) così da evitare intrusioni o scippi di dati sul fronte social;
- Mantenere la "app" costantemente aggiornata alla sua ultima versione;
- Se utilizzate una video-lezione con condivisione dello schermo, è opportuno sapere che tutti potrebbero vedere il desk del vostro pc quando riducete l'app ad icona (es.: chi condivide con voi il vostro schermo, gli studenti, possono visualizzare le altre chat o chiamate, mail in arrivo, documenti da consultare magari proprio per la discussione o la didattica in corso, il desktop del vostro pc, i file aperti, etc.).

Antivirus (regole generali)

- Aggiornare regolarmente il programma antivirus installato;
- Non aprire, sia quando si lavora in rete che quando lo strumento è utilizzato in locale, files sospetti e di dubbia provenienza;
- Non scaricare o installare applicazioni/software che non siano state preventivamente approvate e autorizzate o comunque non ritenute o che non ritieni sicure;
- Verificare, con l'ausilio del programma antivirus in dotazione, ogni supporto magnetico contenente dati prima dell'esecuzione dei file in esso contenuti;
- In caso di ricevimento di e-mail con allegati, verificare anteriormente all'apertura del file l'indirizzo di posta elettronica del mittente, con particolare riguardo al dominio (quindi verificando che non vi siano lettere o numeri anomali);
- Non utilizzare supporti esterni, inclusi CD o chiavette USB, di provenienza incerta;
- Di seguito alcuni brevi cenni sulla procedura da adottare in caso di sospetta presenza di un virus, ad esempio:
- sospendere ogni operazione sul PC, evitando di lavorare con il sistema infetto;
- contattare immediatamente l'Area IT;
- chiudere il sistema e le relative applicazioni

Protezione dei dispositivi portatili

- L'obbligo di ricoverare il dispositivo in un luogo sicuro alla fine della giornata lavorativa;
- Il divieto di lasciarlo incustodito;
- Il divieto di conservare file in locale o, in caso di necessità di rendere la prestazione offline (quindi di impossibilità di accesso al server aziendale o al cloud), la raccomandazione di conservare solo i documenti strettamente necessari all'espletamento della mansione e di provvedere al loro upload nel sistema dell'istituto e alla cancellazione dal dispositivo non appena riottenuto l'accesso ad internet;
- In caso di furto o smarrimento, l'obbligo di immediato avviso al titolare del trattamento o all'Area IT, onde attivare le necessarie procedure di "Data Breach";
- L'obbligo di utilizzare la massima diligenza e operare con la massima riservatezza quando si utilizzano sistemi informatici ed elettronici in pubblico, onde evitare che dati o password possano essere intercettati da soggetti terzi.