AGENZIA FORMATIVA
della PROVINCIA di VARESE

Regolamento per il corretto utilizzo dei dati, di internet, della posta elettronica e delle risorse informatiche e telematiche

(adeguamento previsioni Garante per la protezione dei dati personali 01/03/2007 e Regolamento UE 2016/679 – GDPR)

Approvato con delibera del Consiglio di Amministrazione n° 3 del 28/01/2020
Modificato con delibera di Consiglio di Amministrazione n° 13 del 23/03/2021

INDICE

Art. 1. Obiettivo del presente documento 1

Art. 2. Norme di carattere generale 1

Art. 3. Utilizzo del Personal computer e degli apparati collegati 2

Art. 4. Utilizzo della rete locale (LAN) 3

Art. 5. Utilizzo della posta elettronica 4

Art. 6. Utilizzo di Internet 5

Art. 7. Utilizzo delle risorse telefoniche 6

Art. 8. Gestione delle password 6

Art. 9. Utilizzo dei supporti di memorizzazione 8

Art. 10. Protezione antivirus 8

Art. 11. Soggetti preposti alla verifica della corretta applicazione e dell'ottemperanza al presente regolamento 9

Art. 1. Obiettivo del presente documento

1.1 Obiettivo del presente documento è assicurare che l'utilizzo di internet, della posta elettronica e più in generale delle risorse informatiche e telematiche dell'Agenzia Formativa della Provincia di Varese avvenga in conformità a quanto prescritto dal Provvedimento del Garante per la protezione dei dati personali del 1 marzo 2007, nonché in conformità a quanto prescritto dal nuovo Regolamento Europeo sulla protezione dei dati, Regolamento UE 2016/679, detto anche "GDPR", da "General Data Protection Regulation".

1.2 Il presente documento contiene una serie di norme e disposizioni di carattere operativo, finalizzate ad assicurare che l'utilizzo delle risorse informatiche e telematiche dell'Agenzia Formativa della Provincia di Varese avvenga in modo corretto, sicuro, efficiente ed efficace e senza aggravio di costi per l'Ente.

Art. 2. Norme di carattere generale

2.1 Tutti gli strumenti e le risorse (personal computer, apparati vari, tra cui penne USB, posta elettronica, accesso ad Internet, accesso alla rete, etc.) sono di proprietà dell'Agenzia Formativa della Provincia di Varese, pertanto ne deve essere fatto un utilizzo a fini esclusivamente lavorativi, coerente e motivato dagli specifici compiti affidati e dal ruolo ricoperto. Deve essere evitato qualsiasi utilizzo personale oppure non chiaramente riconducibile al proprio ruolo e alle proprie mansioni lavorative. Sono di proprietà dell'Agenzia Formativa della Provincia di Varese tutte le mail in ingresso ed in uscita, nonché tutti i files memorizzati su hard disk, su server di rete e più in generale su qualsiasi supporto di memorizzazione. In caso di cessazione o interruzione, anche temporanea, del rapporto di lavoro, è fatto tassativo divieto al dipendente o collaboratore di cancellare qualsiasi messaggio di posta elettronica, sia in ingresso che in uscita, e qualsiasi tipo di file o informazione, anche su supporto cartaceo.

2.2 L'Agenzia Formativa della Provincia di Varese potrà verificare o far verificare da soggetti incaricati lo stato di utilizzo e accedere al contenuto degli strumenti e delle risorse concesse in uso (compresi personal computer, anche portatili, hard disk, cartelle di rete, posta elettronica, siti internet visitati, etc.), per verificarne il corretto ed efficiente utilizzo e per verificare che l'utilizzo avvenga in ottemperanza alle presenti disposizioni operative e per fini strettamente lavorativi.

2.3 L'utilizzo degli strumenti e delle risorse deve essere improntato a criteri di sicurezza, efficienza, efficacia ed economicità, evitando sprechi ed evitando di causare attività non necessarie a carico dell'Agenzia Formativa della Provincia di Varese.

2.4 In caso di dubbio, oppure in caso di poca chiarezza o insufficienza delle istruzioni ricevute, bisogna astenersi dall'intraprendere azioni in autonomia, che anche in buona fede potrebbero comportare danni, disservizi o malfunzionamenti, ed è invece necessario chiedere istruzioni alla Direzione Generale.

Art. 3. Utilizzo del Personal computer e degli apparati collegati

3.1 Il PC e qualsiasi programma applicativo deve essere sempre protetto da password iniziale di accesso, lunga almeno otto caratteri contenente almeno un numero ed un carattere speciale, dovrà essere modificata autonomamente da parte dell'utente finale (assegnatario del PC) almeno ogni sei mesi e in ogni caso (certezza o anche semplice sospetto) in cui la password abbia perso la segretezza. L'accesso iniziale deve avvenire esclusivamente con la propria user-id (e ovviamente con la relativa password), assegnata dall'Agenzia Formativa della Provincia di Varese all'utente. Non è permesso accedere con altre user-id, differenti da quella assegnata.

3.2 Il PC deve esser essere protetto da blocca-schermo con password, che deve attivarsi automaticamente dopo al massimo dieci minuti o meno di inattività, oppure tramite combinazione di tasti <simbolo di Windows> - L, attivata volontariamente dall'utente prima di allontanarsi dal PC.

3.3 Alla fine dell'attività lavorativa il PC deve essere spento, ed è necessario attendere e constatare l'effettivo regolare spegnimento.

3.4 Le configurazioni hardware e software del PC non devono essere per nessun motivo modificate. In caso di effettiva necessità, deve esserne fatta richiesta alla Direzione Generale. In particolare non è consentito installare o disinstallare autonomamente periferiche o apparati e non è consentita l'installazione o la disinstallazione autonoma di programmi.

3.5 E' esplicitamente vietato installare o usare programmi di accesso o controllo remoto senza preventiva autorizzazione da parte della Direzione Generale, ed è esplicitamente vietato installare o usare programmi ~~o~~ che permettano comunque di intercettare le comunicazioni di altri utenti o di accedere ai PC

degli altri utenti. La non ottemperanza può integrare uno o più dei seguenti reati o illeciti:

- accesso abusivo ad un sistema informatico o telematico (art. 615ter C.P.)
- violazione, sottrazione e soppressione di corrispondenza (art. 616 C.P.)
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617quater C.P.)
- installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche.

Art. 4. Utilizzo della rete locale (LAN)

4.1 La rete locale (chiamata anche "LAN" – Local Area Network) è un mezzo che permette di condividere risorse, come ad esempio aree di memorizzazione su server, stampanti, plotter, altri PC, etc.

4.2 In linea generale, tranne eccezioni ben individuate e motivate, tutti i documenti (quindi non solo quelli "ufficiali", ma anche quelli di lavoro o le bozze) devono essere memorizzati esclusivamente nelle cartelle di rete su server o nell'area in cloud scelta e messa a disposizione dall'Agenzia Formativa della Provincia di Varese, e non in locale sul proprio PC. In questo modo ne viene assicurato il regolare salvataggio, e quindi la possibilità di ripristino in caso di necessità; viene inoltre assicurato che i documenti saranno accessibili solo ai soggetti o agli uffici autorizzati, con i corretti permessi di accesso (es. sola lettura, controllo completo, etc.), nonché la necessaria protezione antivirus.

4.3 Nel caso vi siano stampanti di rete collocate in aree distanti, è necessario porre particolare attenzione al fatto che le stampe potrebbero essere generate in aree o in contesti accessibili al pubblico o a soggetti – anche interni – non autorizzati; quindi è necessario ritirare prontamente le stampe dal vassoio di stampa.

4.4 Nel caso vi siano errori o interruzioni delle stampe fatte in rete, talvolta può convenire cancellare la stampa, in quanto la ripresa o la riattivazione della stampante potrebbe avvenire successivamente, anche il giorno dopo, in momenti di non presenza del diretto interessato (l'utente che ha lanciato la stampa) e quindi i documenti potrebbero essere visti o raccolti da personale estraneo o non autorizzato o titolato; quanto appena detto è particolarmente importante e significativo nel caso di documenti con contenuto riservati o confidenziali (es. documenti riguardanti i dipendenti o gli studenti) o contenenti dati sensibili o giudiziari o comunque riservati.

4.5 E' vietato collegare alla rete PC, PC portatili, stampanti, plotter e qualsiasi tipo di apparato, poiché potrebbe compromettere la sicurezza e l'operatività della rete e delle risorse ad essa collegate. In caso di necessità il collegamento deve essere richiesto ed autorizzato dalla Direzione Generale.

Art. 5. Utilizzo della posta elettronica

5.1 La persona assegnataria della casella di posta elettronica è responsabile del suo corretto utilizzo. Nel caso di caselle di posta elettronica affidate in uso ad un gruppo di dipendenti, ciascuno dei dipendenti appartenenti al gruppo è tenuto ad un corretto utilizzo della casella.

5.2 E' vietato utilizzare qualsiasi indirizzo di posta elettronica con dominio internet riconducibile all'Agenzia Formativa della Provincia di Varese per iscriversi o partecipare a forum, gruppi di discussione, mailing list, etc. se non nei casi autorizzati per iscritto dalla Direzione, per esigenze lavorative. E' vietato inoltre rispondere o comunque partecipare alle c.d. "catene di S. Antonio", soprattutto nei casi che descrivano situazioni di bisogno o "commoventi". E' vietato inoltre utilizzare la posta elettronica per inviare comunicazioni del tipo "è nato il figlio di…", "invito alla cena …", "si sposa … raccogliamo soldi per il regalo", etc.

5.3 E' vietato rispondere ai messaggi di "spam", e a tutti i messaggi di origine ignota o dubbia, che richiedano di rispondere al messaggio di posta elettronica inviato o di confermarne la correttezza. Si ricorda che il sistema antispam è "euristico", quindi non infallibile, per cui potrebbero venire bloccate alcune mail (i cosiddetti "falsi positivi") che in realtà non sono spam. In questo caso Agenzia Formativa della Provincia di Varese è sollevata da qualsiasi responsabilità.

5.4 E' necessario porre particolare attenzione prima di aprire messaggi di provenienza dubbia o inattesa, in quanto potrebbero contenere virus o codici maligni; in particolare non bisogna aprire allegati con suffisso .EXE o .BAT, e quelli con un doppio suffisso (es. .VBS.BAT) perché molto probabilmente contengono virus. In questi casi bisogna avvertire la Direzione Generale che attiverà i controlli necessari. Si ricorda comunque che – sebbene più raramente – anche messaggi di posta elettronica provenienti da indirizzi conosciuti possono contenere virus.

5.5 Si ricorda, come già detto all'art.2 del presente documento, che l'indirizzo di posta elettronica assegnato è di esclusiva proprietà dell'Agenzia Formativa

della Provincia di Varese e il suo utilizzo è solo per fini lavorativi e non anche privati.

Art. 6. Utilizzo di Internet

6.1 Come le altre risorse, il collegamento ad Internet deve essere utilizzato esclusivamente per finalità lavorative e non personali; in particolare è vietato scaricare musica, film, e nello specifico, qualsiasi contenuto che sia coperto da diritto d'autore; parimenti è vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi esplicitamente autorizzati dalla Direzione indispensabili per lo svolgimento delle mansioni assegnate (es. remote banking per la disposizione di bonifici).

6.2 E' vietato scaricare e/o installare programmi di qualsiasi tipo (a pagamento, freeware, shareware, etc.) se non nei casi autorizzati dalla Direzione Generale.

6.3 E' esplicitamente vietato visitare siti internet a contenuto erotico, pedo-pornografico, violento, razzista. E' altresì vietato visitare siti di "hacker", in quanto in questo caso vi è una forte probabilità che il computer venga infettato da virus e codici maligni, oppure diventi vittima di programmi di tipo "trojan horse", che potrebbero causare gravi disservizi al PC, alla rete, e agli altri PC in rete.

6.4 E' vietata la partecipazione a forum non professionali e a bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

6.5 L' Agenzia Formativa della Provincia di Varese potrà applicare per singoli e gruppi di utenti politiche di navigazione personalizzate in base alle mansioni ed eventuali disposizioni concordate con il Titolare, al fine di ottimizzare l'uso delle risorse e le prestazioni delle connessioni esistenti, tenendo conto delle esigenze delle varie tipologie di utenti.

6.6 L' Agenzia Formativa della Provincia di Varese potrà effettuare controlli sui siti internet visitati, sui tempi e sulle modalità di collegamento, al fine di individuare eventuali abusi e verificare l'ottemperanza alle presenti disposizioni operative. Gli eventuali controlli saranno comunque effettuati in modo non sistematico, in ottemperanza ai principi di necessità, non eccedenza e proporzionalità e in ogni caso in ottemperanza a quanto prescritto dal Provvedimento del Garante per la protezione dei dati personali dedicato all'utilizzo di internet e della posta elettronica.

Art. 7. Utilizzo delle risorse telefoniche

7.1 Come le altre risorse, anche il telefono, il fax e più in generale tutti gli apparati di telecomunicazione devono essere utilizzati per finalità lavorative e non personali, secondo principi di efficienza ed economicità dell'utilizzo delle risorse.

7.2 Nel caso siano disponibili differenti modalità di comunicazione, deve essere utilizzata la modalità più conveniente, tenendo conto anche dei costi collegati.

7.3 Per verificare l'ottemperanza al presente regolamento, l'Agenzia Formativa della Provincia di Varese potrà tenere traccia delle chiamate effettuate o ricevute da ciascun dipendente, incluso l'orario di chiamata, la durata della conversazione, la numerazione chiamata o chiamante ed il contenuto della comunicazione.

7.4 Nel caso di telefonate anomale (es. eccessivamente lunghe o frequenti), il dipendente è tenuto a fornire indicazioni relativamente alla motivazione della chiamata e/o alle generalità del soggetto chiamante o chiamato.

7.5 In caso di telefonate particolarmente anomale (per durata e/o frequenza), l'Agenzia Formativa della Provincia di Varese potrà accedere a campione al contenuto delle chiamate e più in generale delle comunicazioni effettuate o ricevute.

Art. 8. Gestione delle password

8.1 La password, unitamente alla relativa user-id, costituisce la c.d. coppia di "credenziali di autenticazione", necessarie per accedere a qualsiasi risorsa (PC, programma applicativo, registro elettronico, rete, file, etc.) che debba essere protetta. La user-id è fissa e individua univocamente l'utente assegnatario, come una sorta di "codice fiscale", mentre la password può e deve essere modificata dall'utente periodicamente.

8.2 Le password devono essere tenute segrete e non devono essere comunicate ad altre persone per nessun motivo; nel caso sia necessario condividere un documento o una risorsa con un collega, non si deve comunicare la propria password al collega, ma si devono utilizzare a livello di rete dei meccanismi corretti di condivisione che potranno venire messi in atto facendone richiesta

alla Direzione. Il rivelare la propria password ad altri costituisce reato di comunicazione o diffusione abusiva di codici di accesso a sistemi informatici o telematici, punibile ai sensi dell'art. 615quater del Codice Penale con la reclusione da uno a due anni e con la sanzione amministrativa da Euro 5.164 a Euro 10.329. L'unica eccezione al fatto che la password sia assegnata ed utilizzata su base strettamente personale, è permessa nel caso di accesso a piattaforme web (es. portale di Regione Lombardia – GEFO), nel caso la password sia rilasciata da soggetti (tipicamente Pubbliche Amministrazioni) esterni all'Agenzia.

8.3 La password (e più in generale le password) devono essere modificate ogni sei mesi, e ogni tre mesi nel caso di documenti contenenti dati sensibili o giudiziari. La password deve inoltre essere modificata ogniqualvolta abbia perso la sua segretezza o ve ne sia il sospetto. La mancata modifica delle password con le frequenze richieste costituisce reato di omessa adozione di misure minime di sicurezza, punibile ai sensi dell'art. 83 comma 4 lettera a) del GDPR con la sanzione amministrativa pecuniaria fino a 10.000.000,00 Euro.

8.4 All'atto della modifica, la nuova password deve essere scritta e posta all'interno di una busta chiusa e sigillata, datata e firmata sul lato esterno, e consegnata al soggetto incaricato della custodia delle password (Direttore/Responsabile di sede).

8.5 Per facilitare le operazioni di modifica, è possibile mettere in atto meccanismi automatici che all'approssimarsi della data di scadenza della password producano dei promemoria e ad un certo punto "costringano" l'utente finale a modificare la password.

8.6 Qualora si renda necessario per ragioni tecniche reimpostare la password di accesso (es. nel caso in cui la password venga dimenticata e non sussista la possibilità di accedere a quella depositata (cfr. 8.4)), sarà possibile rivolgersi alla segreteria della sede operativa che provvederà a formalizzare una richiesta di reimpostazione della password all'Help Desk (*helpdesk@agenziaformativa.va.it*), trasmettendo la medesima comunicazione, in copia conoscenza, alla Direzione Generale (*direzione.generale@agenziaformativa.va.it*). L'Help Desk provvederà a rigenerare una nuova password provvisoria, che l'utente dovrà necessariamente modificare al primo accesso provvedendo inoltre ad eseguire nuovamente la procedura di deposito della nuova password prevista al punto 8.4.

8.7 Le password devono essere lunghe almeno otto caratteri contenere 1 numero ed un carattere speciale e non contenere riferimenti agevolmente riconducibili (es. nome) all'utente. Si rammenta che l'utilizzare come password parole di senso compiuto aumenta significativamente i rischi che la password possa venire "indovinata" o scoperta da programmi di "forzatura" delle password, per cui si consiglia di non utilizzare parole di senso compiuto, o almeno di inserire una cifra in qualsiasi posizione.

Art. 9. Utilizzo dei supporti di memorizzazione

9.1 I supporti mobili di memorizzazione (floppy-disk, hard-disk esterni e interni, cd-rom, chiavette USB, etc.) devono essere custoditi con diligenza e scrupolo.

9.2 Le chiavette USB non devono essere mai utilizzate come supporto unico o principale di memorizzazione, ma solo per fare eventuali copie temporanee. I documenti devono sempre e comunque venire memorizzati in via prioritaria sul server di rete.

9.3 Nel caso di utilizzo di chiavette USB, prima di scollegarle del PC devono essere disattivate; se non viene effettuata la disattivazione vi è il forte rischio che tutti i dati contenuti nella chiavetta USB vadano perduti.

9.4 Bisogna porre particolare attenzione ai supporti contenenti informazioni confidenziali o riservate, o dati personali o sensibili: in questo caso, quando i dati non sono più necessari, la cancellazione deve avvenire con modalità che non permettano il successivo recupero. Se trattasi di supporti non riscrivibili, come ad esempio cd-rom, bisogna rendere il supporto inutilizzabile mediante frattura fisica dello stesso.

9.5 I supporti magnetici e cartacei contenenti dati sensibili o giudiziari devono essere custoditi in archivi o contenitori chiusi a chiave o comunque con modalità tali da assicurare la riservatezza dei dati ed evitare che vi sia accesso e conoscenza da parte di soggetti non autorizzati.

Art. 10. Protezione antivirus

10.1 Ciascun utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informativo provocato da virus o da altro software o codice maligno.

10.2 E’ necessario verificare il regolare funzionamento del software antivirus installato, e segnalare immediatamente alla Direzione i casi in cui l’antivirus sia stato disinstallato o non sia funzionante.

10.3 Nel caso il software antivirus rilevi la presenza di un virus, bisogna immediatamente sospendere ogni elaborazione senza spegnere il computer e segnalare l'accaduto al servizio di help desk.

10.4 Non è consentito l'utilizzo di supporti di memorizzazione (es. chiavette USB, cd rom, hard disk esterni etc.) di provenienza ignota. Ogni dispositivo di memorizzazione di provenienza esterna dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, si dovrà avvertire immediatamente il servizio di Help Desk telefonicamente e/o mediante e-mail all’indirizzo helpdesk@agenziaformativa.va.it. L’Help Desk provvederà a coordinarsi con la Direzione per le necessità connesse al registro delle violazioni dei dati.

Art. 11. Soggetti preposti alla verifica della corretta applicazione e dell’ottemperanza al presente regolamento

11.5 La responsabilità di vigilare sulla corretta applicazione e sull’ottemperanza alle presenti disposizioni operative è affidata al Responsabile della protezione dei dati designato ai sensi dell’art. 37 del GDPR e alla Direzione Generale.

11.6 La verifica dell’ottemperanza alle presenti disposizioni operative potrà venire effettuata anche con controlli e ispezioni a campione o su segnalazione o richiesta della Direzione Generale.